Lucent Technologies
Bell Labs Innovations

TAOS

RADIUS Guide and Reference

Part Number: 7820-0729-001
March, 2000

Copyright© 2000 Lucent Technologies. All Rights Reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Lucent Technologies.

For permission to reproduce or distribute, please email your request to techpubs@ascend.com.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

4ESS, 5ESS, A Network of Expertise, AnyMedia, AqueView, AUDIX, B-STDX 8000, B-STDX 9000, ...Beyond Compare, CaseView, Cajun, CajunDocs, CAJUNVIEW, Callmaster, CallVisor, CBX 500, CellPipe, ChoiceNet, ClearReach, ComOS, cvMAX, DACScan, Dacsmate, Datakit, DEFINITY, Definity One, DSL MAX, DSL Terminator, DSLPipe, DSLTNT, Elemedia, Elemedia Enhanced, EMMI, End to End Solutions, EPAC, ESS, EVEREST, Gigabit-scaled campus networking, Globalview, GRF, GX 250, GX 550, HyperPATH, Inferno, InfernoSpaces, Intragy, IntragyAccess, IntragyCentral, Intuity, IP Navigator, IPWorX, LineReach, LinkReach, MAX, MAXENT, MAX TNT, Multiband, Multiband PLUS, Multiband RPM, MultiDSL, MultiVoice, MultiVPN, Navis, NavisAccess, NavisConnect, NavisCore, NavisRadius, NavisXtend, NetCare, NetLight, NetPartner, OneVision, Open Systems Innovations, OpenTrunk, P550, PacketStar, PathStar, Pinnacle, Pipeline, PMVision, PortMaster, SecureConnect, Selectools, Series56, SmoothConnect, Stinger, SYSTIMAX, True Access, WaveLAN, WaveMANAGER, WaveMODEM, WebXtend, and Where Network Solutions Never End are trademarks of Lucent Technologies. Advantage Pak, Advantage Services, AnyMedia, ...Beyond Compare, End to End Solutions, Inter.NetWorking, MAXENT, and NetWork Knowledge Solutions are service marks of Lucent Technologies. Other trademarks, service marks, and trade names mentioned in this publication belong to their respective owners.

Limited Warranty

Lucent Technologies provides a limited warranty to this product. See the warranty document included in your product package.

Ordering Information

To order copies of this document, contact your Lucent Technologies representative or reseller.

Support Telephone Numbers

For a menu of support and other services, call (800) 272-3634. Or call (510) 769-6001 for an operator.

Feedback

Lucent appreciates your comments, either positive or negative, about this manual. Please send them to techpubs@ascend.com.

Lucent Technologies

Customer Service

Customer Service provides a variety of options for obtaining information about Lucent products and services, software upgrades, and technical assistance.

Finding information and software on the Internet

Visit the Web site at `http://www.lucent/com/ins` for technical information, product information, and descriptions of available services.

Visit the FTP site at `ftp.ascend.com` for software upgrades, release notes, and addenda to this manual.

Obtaining technical assistance

You can obtain technical assistance by telephone, email, fax, modem, or regular mail, as well as over the Internet.

Enabling Lucent to assist you

If you need to contact Lucent for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model
- Software and hardware options
- Software version
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your line
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

Calling Lucent from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or an Advantage service contract, or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-2763 to reach the Priority Call queue. The charge of $2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than 3 minutes.

Advantage Services

Advantage Services is a comprehensive selection of services. Installation services help get your Lucent Wide Area Network (WAN) off to the right start. Ongoing maintenance and

support services provide hardware and software solutions to keep your network operating at peak performance. For more information, call (800) 272-3634, or access the Web site at `http://www.lucent/com/ins` and select Services and Support, then Advantage Services.

Other telephone numbers

For a menu of Lucent's services, call (800) 272-3634. Or call (510) 769-6001 for an operator.

Calling Lucent from outside the United States

You can contact Lucent by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

For the Asia Pacific Region, you can find additional support resources at `http://apac.ascend.com.`

Obtaining assistance through correspondence

Lucent maintains two email addresses for technical support questions. One is for customers in the United States, and the other is for customers in Europe, the Middle East, and Asia. If you prefer to correspond by fax, BBS, or regular mail, please direct your inquiry to Lucent's U.S. offices. Following are the ways in which you can reach Customer Service:

- Email from within the U.S.—support@ascend.com
- Email from Europe, the Middle East, or Asia—EMEAsupport@ascend.com
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302

Write to Lucent at the following address:

Attn: Customer Service
Lucent Technologies
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

Contents

Customer Service iii

About This Guide ix

What is in this guide ix
What you should know ix
Documentation conventions x

Chapter 1 Setting Up the TAOS Unit For RADIUS 1-1

Overview of configuration tasks 1-1
Setting up the TAOS unit to communicate with RADIUS 1-1
Required steps for configuring the unit to communicate with RADIUS 1-2
Required configuration tasks at the CLI 1-2
Required configuration tasks at the VT100 interface 1-2
Optional steps for configuring the unit to communicate with RADIUS 1-3
Specifying the duration of a RADIUS timeout 1-4
Specifying the message resulting from a RADIUS timeout 1-4
Specifying whether the unit must return to using the primary RADIUS server 1-5
Specifying whether remote users are dropped with no host for immediate login 1-5
Specifying whether the unit sends values for attributes 6 and 7 to RADIUS 1-6
Specifying how the system behaves when Service-Type (6) is not received 1-6
Specifying the manner in which the unit handles the User-Name attribute 1-7
Configuring Vendor-Specific Attribute (VSA) support 1-8
Limiting excess RADIUS traffic 1-9
Fine-tuning the interaction between the TAOS unit and RADIUS 1-9
Specifying whether to customize the User-Name string (CLI only) 1-10
Configuring distinct ID sequences for packet IDs (CLI only) 1-10
Specifying whether RADIUS authenticates a Telnet session (VT100 only) 1-11
Specifying console port security (VT100 only) 1-11
Specifying information about the host running the APP Server (VT100 only) 1-11
Configuring the unit to recognize a security-card server (VT100 only) 1-11
Specifying a RADIUS bootup server (VT100 only) 1-11
Example of configuring the unit to communicate with RADIUS 1-12
Sample CLI configuration 1-13
Sample VT100 configuration 1-14
Setting up system-wide RADIUS accounting 1-14
Required system-wide accounting configuration tasks 1-14
Required system-wide accounting configuration tasks at the CLI 1-15
Required system-wide accounting configuration tasks at the VT100 interface 1-15
Optional system-wide accounting tasks 1-15
Specifying the source for RADIUS accounting requests 1-16
Specifying a timeout value 1-16
Specifying a retry limit 1-16

Specifying the interval for sending session reports 1-17
Specifying the numeric base for the session ID 1-17
Specifying the reset time 1-18
Specifying whether to send Stop packets with no user name 1-18
Specifying whether to send a second RADIUS Accounting Start record 1-19
Specifying whether to send Stop packets when authentication fails (CLI only) 1-19
Generating accounting IDs on the basis of the source port number (CLI only) 1-19
Specifying the interval for sending checkpoint records (VT100 only) 1-19
Example of setting up system-wide RADIUS accounting 1-20
Sample CLI configuration 1-20
Sample VT100 configuration 1-21
Setting up accounting on a per-user basis 1-22
Overview of per-user accounting attributes 1-22
Specifying per-user accounting attributes 1-23
Example of setting up per-user accounting 1-24
Setting up accounting with dynamic IP addressing 1-25
CLI configuration 1-25
VT100 configuration 1-25
Classifying user sessions in RADIUS 1-26
Using the Class attribute 1-26
Using the Ascend-Number-Sessions attribute 1-26
Generating periodic accounting requests 1-27
CLI configuration 1-27
VT100 configuration 1-27
Example of classifying user sessions 1-27

Chapter 2 Understanding RADIUS Authentication 2-1

Introduction 2-1
RADIUS profile formats 2-1
Pre-authentication 2-2
RADIUS password handling 2-3
Reserved RADIUS passwords 2-3
Password expiration 2-4
The DEFAULT user profile 2-5
Shared secrets and secure exchanges 2-5
Authenticating framed protocol sessions 2-5
Specifying an authentication protocol required for dial-in calls 2-6
How PAP works 2-6
How CHAP and MS-CHAP work 2-6
Requesting a protocol for use in dial-out calls 2-7
Token-card authentication 2-8
Enhanced security with token cards 2-8
A simple method of authenticating token-card calls 2-9
Authenticating token-card connections from TAOS units 2-10
Using PAP-TOKEN authentication 2-10
Using PAP-TOKEN-CHAP authentication 2-11
Using CACHE-TOKEN authentication 2-12
Using ACE authentication for network users 2-13
Tunnel authentication 2-14
Authenticating ATMP tunnels 2-14
Authenticating L2TP tunnels 2-15
Tunnel attribute sets with tags and preferences 2-15

Overview of attribute sets and tags 2-16
Supported tunnel protocols 2-16
Tunnel attributes used with tags 2-17
Example of reordering sets using Tunnel-Preference 2-18
Callback after authentication 2-19

Chapter 3 Understanding RADIUS Accounting 3-1

What is RADIUS accounting? 3-1
What kinds of packets does RADIUS accounting use? 3-1
Accounting Start packets 3-2
Accounting Stop packets 3-2
RADIUS attributes in Start records 3-2
RADIUS attributes in Stop records 3-4
RADIUS attributes in Failure-to-start records 3-10
Proxy RADIUS accounting 3-11
How proxy RADIUS accounting works 3-11
Contents of the Stop record sent by proxy 3-12
Sample accounting records 3-13
A Pipeline unit dialing into a MAX TNT unit 3-14
A modem calling into a MAX unit 3-15
An immediate-modem dialout connection 3-16
A Stop record sent by proxy 3-17

Chapter 4 Reference to RADIUS Attributes 4-1

RADIUS attribute descriptions listed alphabetically 4-1
Free-RADIUS attributes and their RFC equivalents 4-170
RFC-standard attributes not supported by TAOS 4-171
Unused attributes 4-171
Outdated attributes 4-172

Appendix A Contents of RADIUS Packets A-1

Access-Request (1) A-2
Access-Accept (2) A-3
Access-Reject (3) A-8
Access-Password-Request (7) A-8
Access-Password-Ack (8) A-9
Access-Password-Reject (9) A-9
Access-Challenge (11) A-9
Access-Password-Expired (32) A-9
Ascend-Access-Event-Request (33) A-9
Ascend-Access-Event-Response (34) A-9
Ascend-Disconnect-Request (40) A-10
Ascend-Disconnect-Ack (41) A-10
Ascend-Disconnect-Nak (42) A-10
Ascend-Change-Filters-Request (43) A-10
Ascend-Change-Filters-Ack (44) A-10
Ascend-Change-Filters-Nak (45) A-10

Appendix B Sample RADIUS Users File B-1

Appendix C Disconnect/Progress Code Combinations C-1

Index Index-1

About This Guide

What is in this guide

This guide provides detailed information about how to set up the TAOS unit to use the RADIUS (Remote Authentication Dial-In User Service) server. It also contains a complete reference to RADIUS attributes.

Note: This manual describes the full set of features for TAOS units running software version 8.0.0. Some features might not be available with earlier versions or specialty loads of the software.

Warning: Read the safety instructions in the hardware installation guide before installing the product

What you should know

This guide is intended for the person who will configure and maintain RADIUS and the TAOS unit. To use it effectively, you must have a basic understanding of TAOS security and configuration, and be familiar with authentication servers and networking concepts.

While this guide attempts to provide enough conceptual framework to enable an administrator who is not an expert in a particular network technology to configure RADIUS accurately, it does not start from the beginning with any network management topic. Following are the general areas in which it is helpful have some existing knowledge when configuring RADIUS:

- Dial-in LAN connections
- Connection cost management and accounting
- Modems
- Frame Relay
- NetWare and IPX routing
- IP routing
- Domain Name System (DNS)
- Open Shortest Path First (OSPF) routing
- Multicast
- Packet structure and formats (for defining filters)
- Network security

Documentation conventions

Following are the special characters and typographical conventions that might be used in this manual:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
Caution:	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
Warning:	Warns that a failure to take appropriate safety precautions could result in physical injury.
Warning:	Warns of danger of electric shock.

Setting Up the TAOS Unit For RADIUS

1

Overview of configuration tasks 1-1

Setting up the TAOS unit to communicate with RADIUS 1-1

Setting up system-wide RADIUS accounting 1-14

Setting up accounting on a per-user basis 1-22

Setting up accounting with dynamic IP addressing 1-25

Classifying user sessions in RADIUS 1-26

Overview of configuration tasks

In this chapter, you will learn how to set up the TAOS unit to communicate with the RADIUS server, and how to configure RADIUS accounting.

For information about setting up the TAOS unit for RADIUS, see "Setting up the TAOS unit to communicate with RADIUS" on page 1-1. For information about setting up RADIUS accounting, see one or more of the following sections:

- "Setting up system-wide RADIUS accounting" on page 1-14
- "Setting up accounting on a per-user basis" on page 1-22
- "Setting up accounting with dynamic IP addressing" on page 1-25
- "Classifying user sessions in RADIUS" on page 1-26

You can perform each configuration task at the Command-Line Interface (CLI) or at the VT100 interface, depending on the type of TAOS unit you are configuring.

Note: Free RADIUS is not recommended for use with the APX 8000.

Setting up the TAOS unit to communicate with RADIUS

The following sections describe how to set up the TAOS unit to communicate with the RADIUS server. Some of the steps are required. Other settings are optional.

- For a list of required steps, see "Required steps for configuring the unit to communicate with RADIUS" on page 1-2.
- For a list of optional steps, see "Optional steps for configuring the unit to communicate with RADIUS" on page 1-3.

Required steps for configuring the unit to communicate with RADIUS

When configuring the TAOS unit to use RADIUS, you must specify:

- Type of authentication in use
- IP address of at least one RADIUS server
- UDP port number for the daemon
- RADIUS client password

You can have up to three RADIUS servers on your network. One is the primary server. Two additional servers can function as backups. If the primary RADIUS server fails, the TAOS unit automatically contacts the secondary RADIUS server to authenticate a user. When it successfully connects to an authentication server, the TAOS unit uses that machine until it fails to serve requests. By default, the TAOS unit does not revert to using the first host until the second machine fails, even if the first host has come online while the second host is still servicing requests.

Required configuration tasks at the CLI

To use the CLI to specify settings required for RADIUS operation, proceed as follows:

1 In the External-Auth profile, set the Auth-Type parameter to RADIUS.

2 Open the Rad-Auth-Client subprofile.

3 For each Auth-Server parameter, specify the IP address of a RADIUS server.

The TAOS unit first tries to connect to the server specified by Auth-Server-1. If it receives no response within the time specified by the Auth-Timeout parameter, it tries to connect to Auth-Server-2. If it again receives no response within the time specified by Auth-Timeout, it tries to connect to Auth-Server-3. If the TAOS unit's request again times out, it reinitiates the process with Auth-Server-1. The TAOS unit can execute this cycle of requests a maximum of ten times.

If you specify the same address for all three Auth-Server parameters, the TAOS unit keeps trying to create a connection to the same server.

4 Set the Auth-Port parameter to the destination UDP port number on which the RADIUS daemon receives client requests.

5 Set the Auth-Key parameter to the RADIUS client password. The password is case sensitive.

Required configuration tasks at the VT100 interface

To use the VT100 interface to specify settings required for RADIUS operation, proceed as follows:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the Auth menu.

4 Set the Auth parameter to RADIUS.

5 For each Auth Host parameter, specify the IP address of a RADIUS server.

The TAOS unit first tries to connect to the server specified by Auth Host #1. If it receives no response within the time specified by the Auth Timeout parameter, it tries to connect to Auth Host #2. If it again receives no response within the time specified by Auth Timeout, it tries to connect to Auth Host #3. If the TAOS unit's request again times out, it reinitiates the process with Auth Host #1. The TAOS unit can execute this cycle of requests a maximum of ten times.

If you specify the same address for all three Auth Host parameters, the TAOS unit keeps trying to create a connection to the same server.

6 Set the Auth Port parameter to the destination UDP port number on which the RADIUS daemon receives client requests.

7 Set the Auth Key parameter to the RADIUS client password. The password is case sensitive.

Optional steps for configuring the unit to communicate with RADIUS

Depending on your needs, you can set parameters to:

- Specify the duration of a RADIUS timeout.
- Specify the message resulting from a RADIUS timeout.
- Specify whether the TAOS unit must return to using the primary RADIUS server after a timeout.
- Specify whether the TAOS unit drops remote users when no host is specified for immediate login service.
- Specify whether the TAOS unit sends values for the Service-Type (6) and Framed-Protocol (7) attributes to RADIUS.
- Specify how the system behaves when the Service-Type (6) attribute is not received.
- Specify the manner in which the TAOS unit handles the User-Name attribute.
- Configure Vendor-Specific Attribute (VSA) support.
- Limit excess RADIUS traffic.
- Fine-tune the interaction between the TAOS unit and RADIUS.
- Specify whether to customize the User-Name string (CLI only).
- Configure distinct ID sequence spaces for packet IDs (CLI only).
- Specify whether the TAOS unit uses RADIUS to authenticate a Telnet session (VT100 only).
- Specify console port security (VT100 only).
- Specify information about the host running the APP Server utility (VT100 only).
- Configure the unit to recognize a security-card authentication server (VT100 only)
- Specify a RADIUS bootup server (VT100 only).

Specifying the duration of a RADIUS timeout

You can specify the number of seconds the TAOS unit waits for a response to a RADIUS authentication request. If you have a high volume of calls, consider specifying a low value. A high timeout value combined with a high call volume can significantly slow the process of authenticating calls. However, if RADIUS is running on a busy shared UNIX host, or if the RADIUS server is on the remote end of a slow link, consider increasing the timeout value above the default of 1 second.

CLI configuration

In the Rad-Auth-Client subprofile of the External-Auth profile, set the Auth-Timeout parameter to the number of seconds the TAOS unit waits for a response to a RADIUS authentication request. If the TAOS unit does not receive a response within the time you specify, it sends the authentication request to the next server specified by the Auth-Server parameter.

VT100 configuration

In Ethernet > Mod Config > Auth menu, set the Auth Timeout parameter to the number of seconds the TAOS unit waits for a response to a RADIUS authentication request. If the TAOS unit does not receive a response within the time you specify, it sends the authentication request to the next server specified by the Auth Host parameter.

Specifying the message resulting from a RADIUS timeout

By default, if authentication fails on a PPP connection because of a bad password or an authentication server timeout, the Lucent unit gracefully shuts down the PPP connection by sending an LCP-CLOSE request to the dial-up user. If Windows 95 (MSN) receives the LCP-CLOSE during authentication, it displays an invalid-password message. This message is misleading if the failure resulted from a RADIUS timeout. Using the CLI or VT100 interface, you can specify that the message resulting from a RADIUS timeout states that the network failed.

CLI configuration

To specify that the message resulting from a RADIUS timeout states that the network failed, set Disconnect-On-Auth-Timeout=Yes in the Answer-Defaults profile’s PPP-Answer subprofile.

VT100 configuration

To specify that the message resulting from a RADIUS timeout states that the network failed, set Disc On Auth Timeout=Yes in the Ethernet > Answer > PPP-Options menu.

Specifying whether the unit must return to using the primary RADIUS server

If a timeout occurs while the TAOS unit waits for a reply to an authentication request directed to the primary RADIUS server, the TAOS unit sends the authentication request to the secondary RADIUS server. If that fails, the TAOS unit sends the authentication request to the next RADIUS server. By default, if either of the secondary servers acknowledges the request, the TAOS unit continues to use that server instead of the primary one, even if the primary server has come back up. The TAOS unit uses the secondary server until it is no longer available. However, you can specify a limit on the period of time the TAOS unit uses the secondary RADIUS server. At the end of this time period, the TAOS unit sends the next authentication request to the primary RADIUS server.

CLI configuration

To specify the number of seconds the TAOS unit uses the secondary RADIUS server before it sends an authentication request to the primary RADIUS server, set the Auth-Reset-Time parameter in the External-Auth > Rad-Auth-Client subprofile.

VT100 configuration

To specify the number of seconds the TAOS unit uses the secondary RADIUS server before it sends an authentication request to the primary RADIUS server, set the Auth Reset Timeout parameter in the Ethernet > Mod Config > Auth menu.

Specifying whether remote users are dropped with no host for immediate login

If the immediate login service is TCP-Clear or Telnet, and no value is specified for Login-IP-Host in the RADIUS user profile, you can specify whether the TAOS unit drops the connection, or gives the caller access to the terminal-server interface instead. By default, the TAOS unit prevents access to the terminal-server interface when the Login-IP-Host value is not specified, and drops the call.

CLI configuration

To specify that the terminal-server must be secure, accept the default value of Yes for Auth-TS-Secure in the External-Auth > Rad-Auth-Client subprofile. To specify that the dial-in client can have access to the terminal-server interface if no Login-IP-Host value is specified, set Auth-TS-Secure=No.

VT100 configuration

To specify that the terminal-server must be secure, accept the default value of Yes for Auth TS Secure in the Ethernet > Mod Config > Auth menu. To specify that the dial-in client can have access to the terminal-server interface if no Login-IP-Host value is specified, set Auth TS Secure=No.

Specifying whether the unit sends values for attributes 6 and 7 to RADIUS

You can specify whether the TAOS unit sends values for the Service-Type (6) and Framed-Protocol (7) attributes in Access-Request packets to the RADIUS server. While some RADIUS servers require these attributes in authentication requests, other RADIUS servers should not receive them.

If you accept the default, which specifies that the TAOS unit sends Service-Type and Framed-Protocol values, you can restrict the type of user and protocol for each connection. For example, when the TAOS unit sends Service Type and Framed-Protocol for a PPP session, the unit sets Service-Type=Framed-User and Framed-Protocol=PPP for incoming PPP calls.

However, if your RADIUS user profiles enable both framed and unframed users to access PPP, you should specify that the TAOS unit does not send values for Service-Type and Framed-Protocol. When you do so, a framed user dials in using a protocol such as SLIP or MP+. An unframed user makes an asynchronous connection to the terminal server, and can start Telnet, Rlogin, or raw TCP sessions.

CLI configuration

To specify that the TAOS unit sends values for attributes 6 and 7 to RADIUS, set Auth-Send67=Yes in the External-Auth > Rad-Auth-Client subprofile. To specify that the TAOS unit does not values for attributes 6 and 7 to RADIUS, set Auth-Send67=No.

VT100 configuration

To specify that the TAOS unit sends values for attributes 6 and 7 to RADIUS, set Auth Send Attr 6, 7=Yes in the Ethernet > Mod Config > Auth menu. To specify that the TAOS unit does not values for attributes 6 and 7 to RADIUS, set Auth Send Attr 6, 7=No.

Specifying how the system behaves when Service-Type (6) is not received

You can specify how the system behaves when it does not receive the Service-Type value from the RADIUS server.

CLI configuration

To use the CLI to specify how the system behaves when it does not receive the Service-Type attribute, set the NoAttr6-Use-Termsrv parameter in the External-Auth profile:

- Yes specifies that the TAOS unit initiates a terminal-server login if Service-Type is not received, regardless of whether a Framed-Protocol (7) value is received or not.
- No specifies that if Service-Type is not received, but Framed-Protocol is received, a framed-protocol login is initiated. If neither Service-Type nor Framed-Protocol is received, a terminal-server login is initiated.

VT100 configuration

To use the VT100 interface to specify how the system behaves when it does not receive the Service-Type attribute, set the No Attr. 6, Use Termsrv parameter in the Ethernet > Mod Config >Auth menu:

- Yes specifies that the TAOS unit initiates a terminal-server login if Service-Type is not received, regardless of whether a Framed-Protocol (7) value is received or not.
- No specifies that if Service-Type is not received, but Framed-Protocol is received, a framed-protocol login is initiated. If neither Service-Type nor Framed-Protocol is received, a terminal-server login is initiated.

Specifying the manner in which the unit handles the User-Name attribute

The RADIUS server typically returns the User-Name attribute in each Access-Accept packet. When the proxy RADIUS server responds for several RADIUS servers that belong to different organizations, including a User-Name attribute can result in the loss of realm information. You can therefore specify the manner in which the TAOS unit handles the User-Name attribute.

CLI configuration

To use the CLI to specify the manner in which the TAOS unit handles the User-Name attribute, proceed as follows:

1 Make External-Auth > Rad-Auth-Client the working profile.

2 To specify that the User-Name value provided by the server is used for the status display and for RADIUS accounting purposes, accept the default of Change-Name for the Auth-Keep-User-Name parameter. Then, proceed to step 5.

3 To specify that the TAOS unit does not use the User-Name value returned by the server, set Auth-Keep-User-Name=Keep-Name. If a name has been specified, the system uses it. Otherwise, it uses the User-Name sent to the server for authentication. A user authenticated by CLID or DNIS will appear to have the CLID or DNIS number as his or her user name.

4 When the user name sent to the server is a realm, you can specify that the system behaves as though the setting were Keep-Name. To do so, set Auth-Keep-User-Name to Keep-Realm-Name. (If the user name sent to the server is not a realm, the system behaves as though the setting were Change-Name.)

5 To specify the characters that delimit a realm from the user name, set the Auth-Realm-Delimiters parameter. You can specify up to seven characters in any order. If no characters are listed, the system behaves as though Auth-Keep-User-Name were set to Change-Name. The default is `@/\%`.

VT100 configuration

To use the VT100 interface to specify the manner in which the TAOS unit handles the User-Name attribute, proceed as follows:

1 Navigate to the Ethernet > Mod Config > Auth submenu.

2 To specify that the User-Name value provided by the server is used for the status display and for RADIUS accounting purposes, accept the default of Change Name for the Keep User Name parameter. Then, proceed to step 5.

3 To specify that the TAOS unit does not use the User-Name value returned by the server, set Keep User Name=Keep Name. If a name has been specified, the system uses it. Otherwise, it uses the User-Name sent to the server for authentication. A user authenticated by CLID or DNIS will appear to have the CLID or DNIS number as his or her user name.

4 When the user name sent to the server is a realm, you can specify that the system behaves as though the setting were Keep Name. To do so, set Keep User Name to Keep Realm. (If the user name sent to the server is not a realm, the system behaves as though the setting were Change Name.)

5 To specify the characters that delimit a realm from the user name, set the Realm Delimiters parameter. You can specify up to seven characters in any order. If no characters are listed, the system behaves as though Keep User Name were set to Change Name. The default is `@/\%`.

Configuring Vendor-Specific Attribute (VSA) support

In VSA compatibility mode, the TAOS unit uses the Vendor-Specific attribute to encapsulate Lucent vendor attributes and uses the RFC-defined User-Password encryption algorithm.

In the Old compatibility mode (the default), the TAOS unit does not send the Vendor-Specific attribute to the RADIUS server and does not recognize it if the server sends it. In this mode, the system uses the Ascend algorithm of encrypting and decrypting the User-Password attribute, which differs from the RFC-defined algorithm in that it does not null fill the password string to a multiple of 16 bytes before encryption, and it does not use the previous segment's hash to calculate the next intermediate value when the password is longer than 16 bytes.

Because administrators can configure RADIUS for four different purposes, with each function operating independently of the others and possibly interacting with different RADIUS servers (or clients), three separate parameters are provided for specifying whether to operate in the older Ascend compatibility mode or in VSA compatibility mode.

CLI configuration

To use the CLI to configure VSA support, proceed as follows:

1 To enable VSA compatibility mode when the TAOS unit is using RADIUS for authentication and authorization purposes, set Auth-RADIUS-Compat=Vendor-Specific in the Rad-Auth-Client subprofile of the External-Auth profile.

2 To enable VSA compatibility mode when the TAOS unit is acting as a RADIUS server that is able to accept some requests for certain limited purposes (such as to change filters or disconnect a user), set RADIUS-Server-Compat=Vendor-Specific in the Rad-Auth-Client subprofile of the External-Auth profile.

3 To enable VSA compatibility mode when the TAOS unit is using RADIUS for accounting purposes, set Acct-RADIUS-Compat=Vendor-Specific in the Rad-Acct-Client subprofile of the External-Auth profile.

VT100 configuration

To use the VT100 interface to configure VSA support, proceed as follows:

1 To enable VSA compatibility mode when the TAOS unit is using RADIUS for authentication and authorization purposes, set Auth Compat Mode=VSA in the Ethernet > Mod Config > Auth menu.

2 To enable VSA compatibility mode when the TAOS unit is acting as a RADIUS server that is able to accept some requests for certain limited purposes (such as to change filters or disconnect a user), set Compat Mode=VSA in the Ethernet > Mod Config > RADIUS Server menu.

3 To enable VSA compatibility mode when the TAOS unit is using RADIUS for accounting purposes, set Acct Compat Mode=VSA in the Ethernet > Mod Config > Accounting menu.

Limiting excess RADIUS traffic

If you do not use RADIUS pseudo-user profiles, you can direct the TAOS unit to not requests for pseudo-user information.

CLI configuration

To prevent the TAOS unit from sending requests for the configuration information stored in pseudo-user profiles, set Allow-Extern-Config-Rqsts to No in the Rad-Auth-Client subprofile of the External-Auth profile.

VT100 configuration

To prevent the TAOS unit from sending requests for the configuration information stored in pseudo-user profiles, set Allow-Extern-Config-Rqsts to No in the Ethernet > Mod Config > Auth menu.

Fine-tuning the interaction between the TAOS unit and RADIUS

This section describes various settings you can make to fine-tune communication between the TAOS unit and the RADIUS server.

CLI configuration

All the steps that follow set parameters in the External-Auth profile's Rad-Auth-Client subprofile. To fine-tune the interaction between the TAOS unit and RADIUS, proceed as follows:

1 Set the Auth-Pool parameter to specify whether the TAOS unit sends the IP address derived from pool #1 to the RADIUS server during an authentication request.

2 Set Auth-Rsp-Required=Yes to enforce Calling-Line ID (CLID) authentication for connections that require it.

3 Set the Local-Profiles-First parameter to specify whether the TAOS unit first checks for a local Connection profile when attempting to authenticate a connection.

4 Set the Auth-Sess-Interval parameter to specify the interval in seconds at which the TAOS unit sends session reports.

5 Set the Auth-Src-Port parameter to a value representing the TAOS unit's UDP source port for sending RADIUS authentication requests. (You can specify the same value for authentication and accounting requests.)

6 Set the Auth-ID-Max-Retry-Time parameter to specify a maximum time limit for RADIUS CLID or Dialed Number Information Service (DNIS) authentication retries.

VT100 configuration

All the steps that follow set parameters in the Ethernet > Mod Config > Auth menu. To fine-tune the interaction between the TAOS unit and RADIUS, proceed as follows:

1 Set the Auth Pool parameter to specify whether the TAOS unit sends the IP address from pool #1 to the RADIUS server during an authentication request.

2 Set Auth Req=Yes to enforce Calling-Line ID (CLID) authentication for connections that require it.

3 Set the Local Profiles First parameter to specify whether the TAOS unit first checks for a local Connection profile when attempting to authenticate a connection.

4 Set the Sess Timer parameter to specify the interval in seconds at which the TAOS unit sends session reports.

5 Set the Auth Src Port parameter to a value representing the TAOS unit's UDP source port for sending RADIUS authentication requests. (You can specify the same value for authentication and accounting requests.)

6 Set the Auth Id Max Retry Time parameter to specify a maximum time limit for RADIUS CLID or Dialed Number Information Service (DNIS) authentication retries.

Specifying whether to customize the User-Name string (CLI only)

To enable a proxy RADIUS server that does not have the shared secret to distinguish between pseudo-user and real user authentication requests, you can customize the User-Name string presented to the RADIUS server during CLID or DNIS authentication. To do so, specify up to 16 characters for the ID-Auth-Prefix setting in the Rad-Auth-Client subprofile. The specified string is inserted as a prefix to the phone number in CLID or DNIS authentication requests to the RADIUS server. The RADIUS server can then forward different types of requests to different servers.

Configuring distinct ID sequences for packet IDs (CLI only)

RADIUS uses an ID value to aid in Request-Response matching. By default, the TAOS unit uses a single sequence space for the RADIUS ID number in all RADIUS messages, which limits the number of IDs available for assignment to 256. A combined total of 256 authentication and accounting packets are sent before the ID sequence rolls over. However, you can configure distinct ID sequence spaces for RADIUS accounting and authentication packets.

When you configure the TAOS unit to use distinct ID sequence spaces, the RADIUS server must perform additional checks for duplicate detection. The server should check the RADIUS ID value as well as the service type and destination UDP port in each packet. The service type can be determined by sorting all values of the code field into two classes—Auth and Acct—and then comparing the received code value to determine to which class it belongs. The destination UDP port can be the same for both services when a single RADIUS server performs them.

To configure distinct ID sequence spaces for RADIUS accounting and authentication packets, set Rad-ID-Space=Distinct in the External-Auth profile. When you set Rad-ID-Space=Distinct, RADIUS authentication and accounting packets do not share the same ID sequence space. The TAOS unit can send a total of 256 authentication packets before the authentication ID sequence rolls over, and 256 accounting packets before the accounting ID sequence rolls over.

Specifying whether RADIUS authenticates a Telnet session (VT100 only)

To enable the TAOS unit to use a RADIUS server to authenticate a Telnet session, set Telnet Security=Auth in the Ethernet > Mod Config menu. The TAOS unit first attempts authentication with a RADIUS profile. If that fails, the TAOS unit tries to match a Security profile to the login name and password. The TAOS unit allows the user three login attempts before it closes the Telnet session.

Specifying console port security (VT100 only)

To enable the TAOS unit to use a RADIUS server to authenticate a console port user, set Console Security=Auth Setting in the System > Sys Config menu. The TAOS unit first attempts authentication with a RADIUS profile. If that fails, the TAOS unit tries to match a Security profile to the login name and password.The Ascend-Telnet-Profile RADIUS attribute must be set to Full Access or to the name of a valid Security profile.

Specifying information about the host running the APP Server (VT100 only)

To specify information about the host running the APP Server utility, set the APP Server, APP Host, and APP Port parameters in the Ethernet > Mod Config > Auth menu.

Configuring the unit to recognize a security-card server (VT100 only)

To configure the TAOS unit to recognize a security-card authentication server, set the Password Server and Password Port parameters in the Ethernet > Mod Config > Auth menu.

Specifying a RADIUS bootup server (VT100 only)

The TAOS unit can obtain pseudo-user configuration information from a RADIUS server other than the one used for authentication. The RADIUS server containing the pseudo-user information is called a *bootup server.* To configure the TAOS unit to obtain pseudo-user configuration information from a bootup server, proceed as follows:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the Auth menu.

4 For the Auth Boot Host #1 parameter, enter an IP address for the primary bootup server.

5 To specify a backup server that can service requests should the primary server go offline, enter an IP address for the Auth Boot Host #2 parameter.

6 To specify the port number the TAOS unit uses when it contacts the bootup server, set the Auth Boot Port parameter. You can specify a number from 1 to 65535.

7 Save your changes.

Example of configuring the unit to communicate with RADIUS

The configuration illustrated in Figure 1-1 uses three RADIUS servers. Clients dialing in across the WAN use both framed and unframed protocols on analog and digital lines. The RADIUS daemon for each server receives client requests on UDP port 512, and the client password is `mypass`.

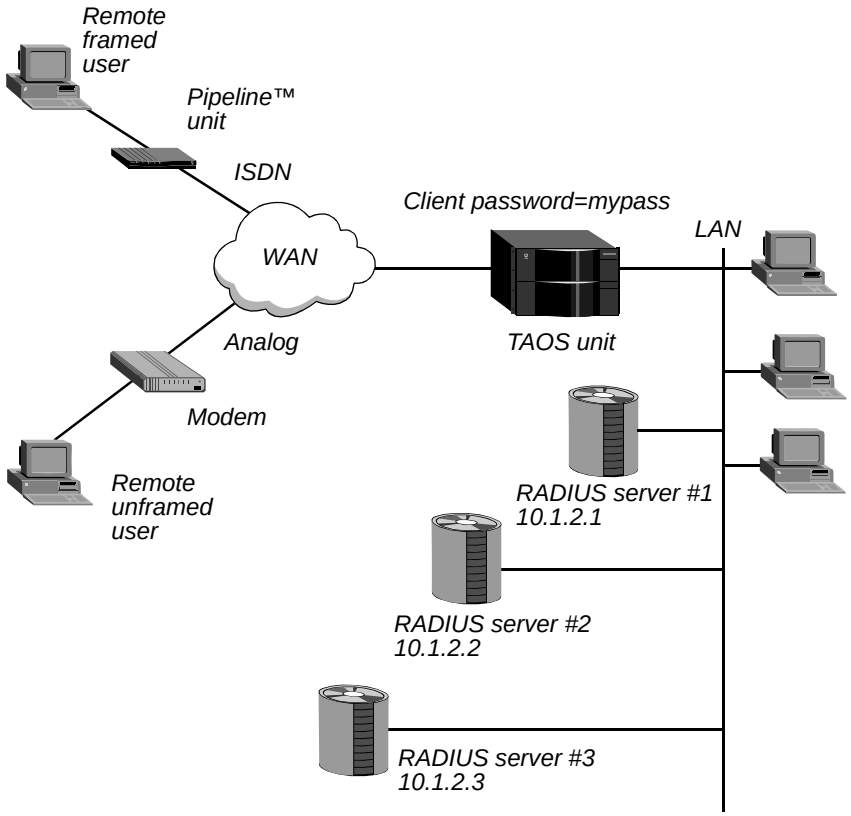


Figure 1-1. Sample network topology for setting up the TAOS unit to use the RADIUS server

In addition to the required parameters, the configuration specifies that the TAOS unit must:

- Enforce CLID authentication for all remote users.
- Check for a RADIUS profile before a local Connection profile.
- Send session reports every 60 seconds.
- Use UDP source port 500 for sending authentication requests.
- Allow both framed and unframed users to access PPP.
- Increase the timeout value to 10 seconds.

Sample CLI configuration

To set the values at the CLI for the sample configuration, you would proceed as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set auth-type=radius

admin> list rad-auth-client
[in EXTERNAL-AUTH:rad-auth-client]
auth-server-1=0.0.0.0
auth-server-2=0.0.0.0
auth-server-3=0.0.0.0
auth-port=0
auth-src-port=0
auth-key=""
auth-pool=no
auth-timeout=0
auth-rsp-required=no
auth-id-fail-return-busy=no
auth-id-timeout-return-busy=no
auth-sess-interval=0
auth-TS-secure=yes
auth-Send67=yes
auth-frm-adr-start=no
auth-boot-host=0.0.0.0
auth-boot-host-2=0.0.0.0
auth-boot-port=0
auth-reset-time=0
auth-id-max-retry-time=0
auth-radius-compat=old-ascend
auth-keep-user-name=change-name
auth-realm-delimiters=/\@%
id-auth-prefix=””

admin> set auth-server-1=10.1.2.1

admin> set auth-server-2=10.1.2.2

admin> set auth-server-3=10.1.2.3

admin> set auth-port=512

admin> set auth-key=mypass

admin> set auth-rsp-required=yes

admin> set local-profiles-first=lpf-no

admin> set auth-sess-interval=60

admin> set auth-src-port=500

admin> set auth-send67=no

admin> set auth-timeout=10

admin> write external-auth
EXTERNAL-AUTH written
```

Sample VT100 configuration

To set the values at the VT100 interface for the sample configuration, you would proceed as follows:

1. Open the Ethernet menu.
2. Open the Mod Config menu.
3. Open the Auth menu.
4. Set Auth to RADIUS.
5. To specify the address of the primary RADIUS server, set Auth Host #1 to 10.1.2.1.
6. To specify the address of the secondary RADIUS server, set Auth Host #2 to 10.1.2.2.
7. To specify the address of the tertiary RADIUS server, set Auth Host #3 to 10.1.2.3.
8. To specify the UDP port on which the RADIUS daemon accepts client requests, set Auth Port to 512.
9. To specify the client password, set Auth Key to `mypass`.
10. To enforce CLID authentication for all remote users, set Auth Req to Yes.
11. To specify that the unit checks for a RADIUS user profile before a local Connection profile, set Local Profiles First to No.
12. To send session reports every 60 seconds, set Sess Timer to 60.
13. To specify the UDP source port for sending authentication requests, set Auth Src Port to 500.
14. To allow both framed and unframed users to access PPP, set Auth Send Attr 6, 7 to No.
15. To increase the timeout values to 10 seconds, set Auth Timeout to 10.
16. Save your changes.

Setting up system-wide RADIUS accounting

The following sections describe how to set up the TAOS unit for system-wide RADIUS accounting. Some of the steps are required. Other settings are optional.

- For a list of required steps, see “Required system-wide accounting configuration tasks” on page 1-14.
- For a list of optional steps, see “Optional system-wide accounting tasks” on page 1-15.

Required system-wide accounting configuration tasks

When you set up system-wide RADIUS accounting, you must perform the following tasks:

- Specify RADIUS accounting.
- Specify the IP address of a RADIUS host.
- Specify a UDP port number.
- Specify the RADIUS client password.

Required system-wide accounting configuration tasks at the CLI

To set accounting parameters that affect all users on a system-wide basis, perform the following steps at the CLI:

1. In the External-Auth profile, set Acct-Type =RADIUS.
2. Open the Rad-Acct-Client subprofile.
3. For each Acct-Server parameter, specify the IP address of a RADIUS host.
4. For the Acct-Port parameter, enter the UDP port number you specified for the authentication process of the daemon.
5. For the Acct-Key parameter, enter the RADIUS client password.

Required system-wide accounting configuration tasks at the VT100 interface

1. Open the Ethernet menu.
2. Open the Mod Config menu.
3. Open the Accounting menu.
4. Set Acct=RADIUS.
5. For each Acct Host parameter, specify the IP address of a RADIUS accounting server.
6. For the Acct Port parameter, enter the UDP port number you specified for the authentication process of the daemon.
7. For the Acct Key parameter, enter the RADIUS client password.

Optional system-wide accounting tasks

Depending on your needs, you can set parameters to:

- Specify the source for RADIUS accounting requests.
- Specify a timeout value.
- Set a retry limit.
- Specify a session-report interval.
- Specify a numeric base for the session ID.
- Specify a reset time.
- Specify whether the TAOS unit send Accounting Stop packets that do not contain a user name.
- Specify whether the TAOS unit generates a second Accounting Start packet when the RADIUS Framed-IP-Address value is assigned.
- Specify whether the TAOS unit sends Accounting Stop packets when a connection fails authentication (CLI only).
- Generate unique accounting IDs on the basis of the source UDP port number of accounting packets (CLI only).
- Specify the interval at which the TAOS unit send checkpoint records for an active user session (VT100 only).

Specifying the source for RADIUS accounting requests

You can specify the UDP source port for sending RADIUS accounting requests. If you wish, you can specify the same value for authentication and accounting requests.

CLI configuration

In the Rad-Acct-Client subprofile of the External-Auth profile, set the Acct-Src-Port parameter to a value representing the TAOS unit's UDP source port for sending RADIUS accounting requests.

VT100 configuration

In the Ethernet > Mod Config > Accounting menu, set the Acct Src Port parameter to a value representing the TAOS unit's UDP source port for sending RADIUS accounting requests.

Specifying a timeout value

You can specify the number of seconds the TAOS unit waits for a response to a RADIUS accounting request.

CLI configuration

In the Rad-Acct-Client subprofile of the External-Auth profile, set the Acct-Timeout parameter to a number from 1 to 10. The default value is 1.

VT100 configuration

In the Ethernet > Mod Config > Accounting menu, set the Acct Timeout parameter to a number from 1 to 10. The default value is 1.

Specifying a retry limit

When the TAOS unit is configured for RADIUS accounting, it sends Accounting Start and Stop packets to the RADIUS server to record connections. If the server does not acknowledge a packet within the number of seconds you specify, the TAOS unit tries again, resending the packet until the server responds, or dropping the packet because the queue is full.

You can specify the maximum number of retries for Accounting packets. The TAOS unit always attempts at least one retry. For example, if you set the number of retries to 10, the TAOS unit makes 11 attempts: the original attempt plus 10 retries.

CLI configuration

In the Rad-Acct-Client subprofile of the External-Auth profile, set the Acct-Limit-Retry parameter to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

VT100 configuration

In the Ethernet > Mod Config > Accounting menu, set the Acct Max Retry parameter to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

Specifying the interval for sending session reports

The TAOS unit can report the number of sessions by class to a RADIUS accounting server. You can specify the interval, in seconds, at which the TAOS unit sends session reports. (For complete information about setting up the TAOS unit for session reports, see “Classifying user sessions in RADIUS” on page 1-26.)

CLI configuration

In the Rad-Acct-Client subprofile of the External-Auth profile, set the Acct-Sess-Interval parameter to a number from 0 to 65535.The default value is 0 (zero), which specifies that the TAOS unit does not send reports on session events.

VT100 configuration

In the Ethernet > Mod Config > Accounting menu, set the Sess Timer parameter to a number from 0 to 65535. The default value is 0 (zero), which specifies that the TAOS unit does not send reports on session events.

Specifying the numeric base for the session ID

The Acct-Session-ID attribute is a unique numeric string identified with the session reported in an Accounting packet. You can control whether the TAOS unit presents Acct-Session-ID to the accounting server in base 10 or base 16. For example, when you specify base 10, the TAOS unit presents a typical session ID to the accounting server in the following format:

```
"1234567890"
```

When you specify base 16, the TAOS unit presents the same session ID in the following format:

```
"499602D2"
```

Note: Changing the value of the numeric base while sessions are active creates inconsistencies between the Start and Stop records.

CLI configuration

Specify one of the following settings:

- Acct-Base-10 (decimal) specifies that the numeric base is 10. The default value is Acct-Base-10.
- Acct-Base-16 (hexadecimal) specifies that the numeric base is 16.

VT100 configuration

Specify one of the following settings:

- 10 (decimal) specifies that the numeric base is 10. The default value is 10.
- 16 (hexadecimal) specifies that the numeric base is 16.

Specifying the reset time

You can specify the number of seconds that must elapse before the TAOS unit returns to using the primary RADIUS accounting server. The default is 0 (zero), which specifies that the TAOS unit does not return to using the primary RADIUS accounting server.

CLI configuration

In the Rad-Acct-Client subprofile of the External-Auth profile, set the Acct-Reset-Time parameter to the number of seconds that must elapse before the TAOS unit returns to using the primary RADIUS accounting server.

VT100 configuration

In Ethernet > Mod Config > Accounting menu, set the Acct Reset Timeout parameter to the number of seconds that must elapse before the TAOS unit returns to using the primary RADIUS accounting server.

Specifying whether to send Stop packets with no user name

At times, the TAOS unit can send an Accounting Stop packet to the RADIUS server without having sent an Accounting Start packet. Such Stop packets have no user name. You can specify that the TAOS unit should not send an Accounting Stop packet that does not contain a user name.

CLI configuration

To specify that the TAOS unit should not send an Accounting Stop packet that does not contain a user name, set Acct-Stop-Only=No in the Rad-Acct-Client subprofile of the External-Auth profile.

VT100 configuration

To specify that the TAOS unit should not send an Accounting Stop packet that does not contain a user name, set Allow Stop Only in the Ethernet > Mod Config > Accounting menu.

Specifying whether to send a second RADIUS Accounting Start record

You can specify that the TAOS unit sends a second RADIUS Accounting Start record when the RADIUS Framed-IP-Address value is assigned.

CLI configuration

To specify that the TAOS unit sends a second RADIUS Accounting Start record when the RADIUS Framed-IP-Address value is assigned, set Auth-Frm-Adr-Start=Yes in the Rad-Acct-Client subprofile of the External-Auth profile.

VT100 configuration

To specify that the TAOS unit sends a second RADIUS Accounting Start record when the RADIUS Framed-IP-Address value is assigned, set Framed Addr Start=Yes in the Ethernet > Mod Config > Auth menu.

Specifying whether to send Stop packets when authentication fails (CLI only)

By default, RADIUS Accounting Stop packets are sent for authenticated connections, connections that are dropped before authenticating, and connections that fail authentication. To configure the TAOS unit not to send Stop packets for connections that fail authentication, set Acct-Drop-Stop-On-Auth-Fail=Yes in the External-Auth > Rad-Acct-Client subprofile.

Generating accounting IDs on the basis of the source port number (CLI only)

RADIUS uses ID values in Request-Response matching. For each unique accounting request (including retries, if a response is not received within the configured timeout period), RADIUS assigns an 8-bit ID value. The assigned value is freed when the request is no longer pending—that is, when RADIUS matches a request with a response, or the request times out.

When the TAOS unit runs at high capacity, RADIUS can run out of unique IDs. To overcome this limitation, you can specify that each request be identified by the UDP source port as well as by the RADIUS ID value.

To specify that the TAOS unit sends the source UDP port number in RADIUS Request-Response matching, accept the default of Rad-ID-Source-Unique=Port-Unique in the External-Auth profile. If you want each request to be identified only by the RADIUS ID value, set Rad-ID-Source-Unique=System-Unique.

Specifying the interval for sending checkpoint records (VT100 only)

To specify the interval in minutes at which the TAOS sends checkpoint records for an active user session, set the Acct Checkpoint parameter to a number from 0 to 60. The default is 0 (zero), which specifies that the TAOS unit send no checkpoint records.

Example of setting up system-wide RADIUS accounting

The configuration illustrated in Figure 1-1 uses three RADIUS accounting servers. Clients dialing in across the WAN use both framed and unframed protocols on analog and digital lines. The RADIUS daemon for each server receives client requests on UDP port 512, and the client password is `mypass`.

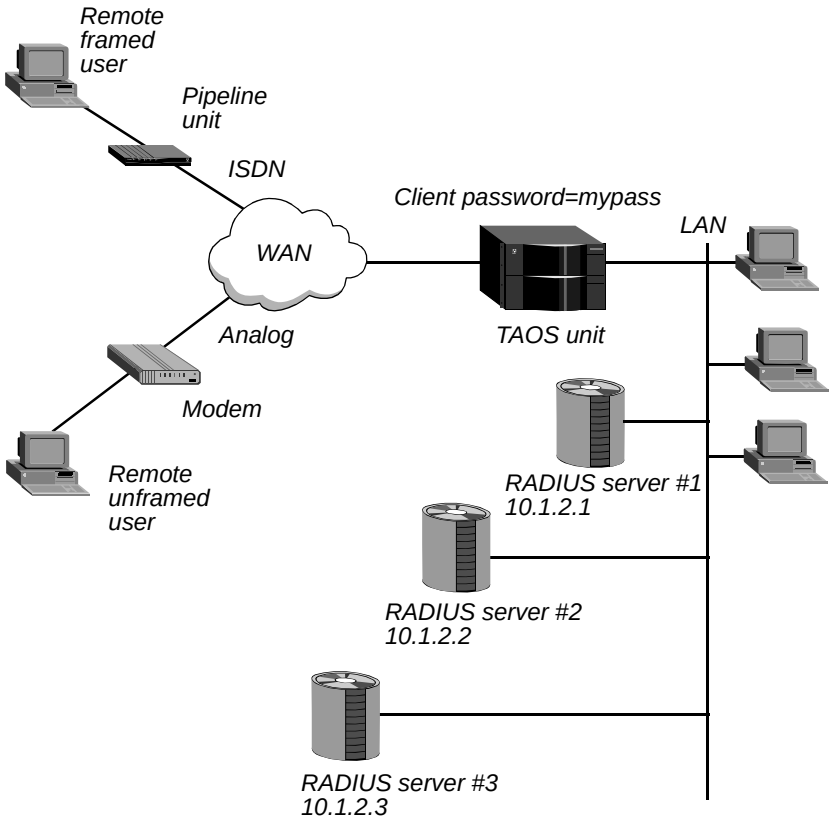


Figure 1-2. Sample network topology for setting up system-wide RADIUS accounting

In addition to the required parameters, the configuration also specifies that the TAOS unit must:

- Use UDP source port 500 for sending accounting requests.
- Increase the timeout value to 10 seconds.
- Increase the retry limit to 6.

Sample CLI configuration

To set the values at the CLI for the sample configuration, you would proceed as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set acct-type=radius
```

```
admin> list rad-acct-client
[in EXTERNAL-AUTH:rad-acct-client (changed)]
acct-server-1=0.0.0.0
acct-server-2=0.0.0.0
acct-server-3=0.0.0.0
acct-port=0
acct-src-port=0
acct-key=""
acct-timeout=0
acct-sess-interval=0
acct-id-base=acct-base-10
acct-reset-time=0
acct-stop-only=yes
acct-limit-retry=0
acct-drop-stop-on-auth-fail=no
admin> set acct-server-1=10.1.2.1
admin> set acct-server-2=10.1.2.2
admin> set acct-server-3=10.1.2.3
admin> set acct-port=512
admin> set acct-src-port=500
admin> set acct-key=mypass
admin> set acct-timeout=10
admin> set acct-limit-retry=6
admin> write external-auth
EXTERNAL-AUTH written
```

Sample VT100 configuration

To set the values at the VT100 interface for the sample configuration, you would proceed as follows:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the Accounting menu.

4 To specify RADIUS accounting, set Acct=RADIUS.

5 To specify the address of the primary accounting server, set Acct Host #1=10.1.2.1.

6 To specify the address of the secondary accounting server, set Acct Host #2=10.1.2.2.

7 To specify the address of the tertiary accounting server, set Acct Host #3=10.1.2.3.

8 To specify the UDP port for receiving client requests, set Acct Port=512.

9 To specify the UDP source port for sending accounting requests, set Acct Src Port=500.

10 To specify the client password, set Acct Key=`mypass`.

11 To increase the timeout value to 10 seconds, set Acct Timeout=10

12 To increase the retry limit to 6, set Acct Max Retry=6.

13 Save your changes.

Setting up accounting on a per-user basis

A network reseller can serve many different ISPs, each with a different access policy. The reseller carries traffic for individual users, and must bill for usage according to the policies of the appropriate ISP. With per-user accounting, a network reseller can direct accounting information about specific users to a RADIUS server belonging to a particular ISP. Each RADIUS user profile can specify that accounting data goes to one or both of the following locations:

- The server specified at the local interface on the TAOS unit. This server is known as the *default server.*

  At the CLI, the default server is specified by the Acct-Server parameter in the External-Auth profile's Rad-Acct-Client subprofile. At the VT100 interface, the default server is specified by the Acct Host parameter in the Ethernet > Mod Config > Accounting menu.
- The RADIUS accounting server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile.

When an accounting event occurs, the TAOS unit sends an accounting message to the specified server. The TAOS unit places each accounting message on a list and waits for an acknowledgment from the RADIUS server. If an acknowledgment does not arrive within the time limit you specify, the TAOS unit resends the accounting message. RADIUS discards the oldest entry on the list when the total number of entries exceeds the maximum.

Overview of per-user accounting attributes

When you set up accounting on a per-user basis, you use the attributes described in Table 1-1.

Table 1-1. Per-user accounting attributes

Attribute	Description	Possible values
Ascend-User-Acct-Base (142)	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.	Ascend-User-Acct-Base-10 (0) Ascend-User-Acct-Base-16 (1) Ascend-User-Acct-Base-10 is the default.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for the link.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-User-Acct-Key (141)	Specifies the RADIUS client password.	Text string. The default value is null.
Ascend-User-Acct-Port (140)	Specifies a destination UDP port number for the connection.	The UDP port number for the authentication process of the daemon.

Table 1-1. Per-user accounting attributes (continued)

Attribute	Description	Possible values
Ascend-User-Acct-Time (143)	Specifies the number of seconds the TAOS unit waits for a response to a RADIUS accounting request. If the TAOS unit does not receive a response within the time specified by Ascend-User-Acct-Time, it sends the accounting request to the next accounting server specified locally on the TAOS unit, to the server specified by Ascend-User-Acct-Host in RADIUS, or both.	Integer from 1 to 10. The default is 1.
Ascend-User-Acct-Type (138)	Specifies the RADIUS accounting server to use for the connection.	Ascend-User-Acct-None (0) specifies that the TAOS unit sends accounting information to the default server. Ascend-User-Acct-User (1) specifies that the TAOS unit sends accounting information to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile. Ascend-User-Acct-User-Default (2) specifies that the TAOS unit sends accounting information both to the RADIUS server specified by the Ascend-User-Acct-Host attribute, and to the default server. Ascend-User-Acct-None is the default.

Specifying per-user accounting attributes

To specify a RADIUS accounting server in a RADIUS user profile:

1. Set up the RADIUS user profile.
2. Set the Ascend-User-Acct-Type attribute to specify the RADIUS accounting server for the connection.
3. Set the Ascend-User-Acct-Host attribute to the IP address of the RADIUS accounting server for the connection.
4. Set the Ascend-User-Acct-Port attribute to the UDP port number you specified for the authentication process.
5. Set the Ascend-User-Acct-Key attribute to the value of the RADIUS client password.
6. Set the Ascend-User-Acct-Base attribute to specify whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16 (optional).

7 Set the Ascend-User-Acct-Time attribute to the number of seconds the TAOS unit waits for a response to a RADIUS accounting request (optional).

If Ascend-User-Acct-Type is set to Ascend-User-Acct-User-Default, the TAOS unit sends two different packets: one to the server specified in the user profile, and one to the default server.

Example of setting up per-user accounting

In Figure 1-3, the TAOS unit sends accounting information to the RADIUS server at 200.250.56.10 for the user Emma. The destination UDP port is 1645, and the RADIUS client password is `mypassword`.

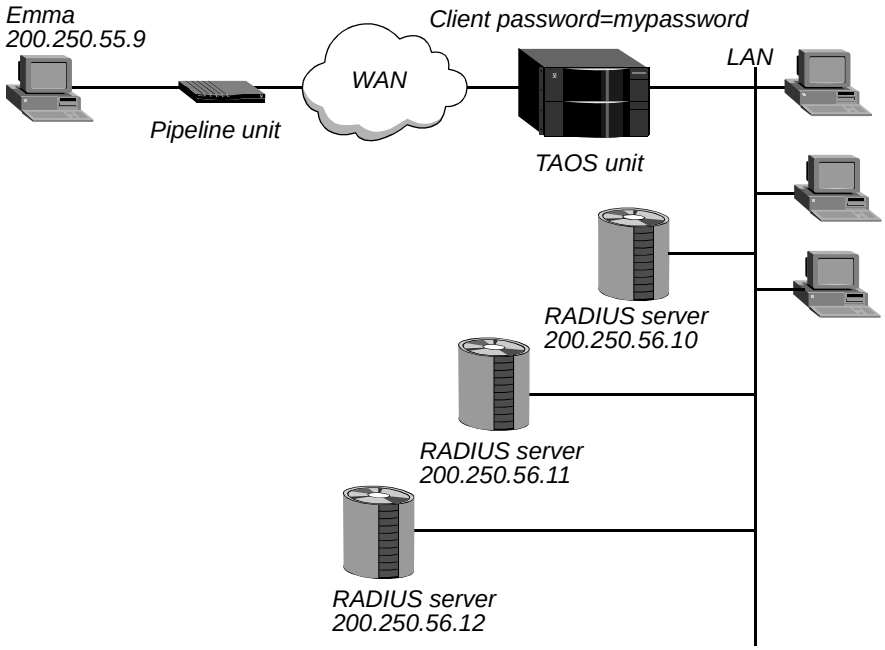


Figure 1-3. Sample network topology for setting up accounting on a per-user basis

To set up per-user accounting for the user Emma, you would configure her user profile as follows:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword"
```

Setting up accounting with dynamic IP addressing

In some networks, the RADIUS accounting server requires an IP address for all callers. For callers that receive an IP address from a pool, this requirement presents a problem. During PPP authentication, RADIUS verifies the name and password, but not the caller's IP address. To track calls during the authentication period, you must set up one or more IP address pools. Then, you must specify whether the TAOS unit includes the caller's assigned IP address as the value of the Framed-Address attribute. The TAOS unit allocates this address from pool #1. (If you do not define pool #1, the call does not have an IP address during authentication.) Because an IP assignment is not usually part of an Access-Request, you must modify the RADIUS daemon.

CLI configuration

In the Rad-Auth-Client subprofile of the External-Auth profile, set Auth-Pool=Yes. When Auth-Pool=Yes, the TAOS unit includes the caller's assigned IP address as the value of the Framed-Address attribute. The assigned IP address might not last the duration of the connection, or it might not be meaningful. Here are five possibilities:

- If Assign-Address=No in the IP-Answer subprofile of the Answer-Defaults profile, and the caller's RADIUS user profile does not supply an IP address for the caller, the TAOS unit returns the IP address to pool #1. However, the address continues to appear in RADIUS accounting entries.
- If Assign-Address=No and the caller's RADIUS user profile supplies an IP address for the caller, the TAOS unit returns the IP address to pool #1. The IP address from the user profile appears in RADIUS accounting entries.
- If Assign-Address=Yes, and Ascend-Assign-IP-Pool in the RADIUS user profile points to a pool that has no valid IP address, the IP address from pool #1 appears in accounting entries. The TAOS unit returns the address to the pool when the call disconnects.
- If Assign-Address=Yes and Must-Accept-Address-Assign=Yes on the TAOS unit, and Ascend-Assign-IP-Pool points to a pool that has a valid IP address, the IP address from that pool appears in RADIUS accounting entries for the duration of the call. The TAOS unit returns the address to the pool when the call disconnects.
- If Assign-Address=Yes, Must-Accept-Address-Assign=No, Ascend-Assign-IP-Pool points to a pool that has a valid IP address, and the caller does not specify an address, the IP address from the pool appears in RADIUS accounting entries. If the caller does specify an IP address, that address appears in RADIUS accounting entries.

VT100 configuration

1. Open the Ethernet menu.
2. Open the Mod Config menu.
3. Open the Auth menu.
4. Set Auth Pool=Yes.
5. Save your changes.

The assigned IP address might not last the duration of the connection or might not be meaningful. Here are five possibilities:

- If Assign Adrs=No and the caller's RADIUS user profile does not supply an IP address for the caller, the TAOS unit returns the IP address to pool #1, but the address continues to appear in RADIUS accounting entries.
- If Assign Adrs=No and the caller's RADIUS user profile does supply an IP address for the caller, the IP address from pool #1 returns to the pool, and the IP address from the user profile appears in RADIUS accounting entries.
- If Assign Adrs=Yes and Ascend-Assign-IP-Pool in the RADIUS user profile points to a pool that has no valid IP address, the IP address from pool #1 appears in RADIUS accounting entries, and returns to the pool only when the call disconnects.
- If Assign Adrs=Yes, Assign Only=Yes, and Ascend-Assign-IP-Pool points to a pool that has a valid IP address, the IP address from that pool appears in RADIUS accounting entries for the duration of the call, and returns to the pool when the call disconnects.
- If Assign Adrs=Yes, Assign Only=No, and Ascend-Assign-IP-Pool points to a pool that has a valid IP address, the IP address from that pool appears in RADIUS accounting entries, unless the caller specifies an address. If the caller specifies an IP address, it appears in RADIUS accounting entries and the IP address derived from the pool is returned.

Classifying user sessions in RADIUS

The Class and Ascend-Number-Sessions attributes enable access providers to classify their user sessions for purposes such as billing clients on the basis of the service option they choose. If you customize RADIUS properly, you can set up the TAOS unit to periodically issue accounting requests.

Using the Class attribute

If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the TAOS unit in the Access-Accept packet when the session begins. Class then appears in Accounting-Request packets the TAOS unit sends to the RADIUS accounting server whenever a session starts and whenever a session stops. The accounting entries specify the class on a per-user and per-session basis.

Using the Ascend-Number-Sessions attribute

The Ascend-Number-Sessions attribute reports information about all user sessions (that is, about the number of current sessions of each class). The attribute has a compound value. The first part indicates a user-session class. The second part reports the number of active sessions in that class. In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.

Generating periodic accounting requests

You can configure the TAOS unit to send accounting requests at regular intervals. At the specified interval, the TAOS unit reports the number of open sessions by sending an Ascend-Access-Event-Request packet (code 33). The packet contains the NAS-IP-Address attribute, followed by a list of Ascend-Number-Sessions attributes.

Only RADIUS daemons you customize to recognize packet code 33 respond to Ascend-Access-Event-Request packets from the TAOS unit. Other accounting daemons ignore it. When modifying the daemon, make sure that it recognizes the following format for an Ascend-Access-Event-Request packet:

```
Code (8-bit)=33
Identifier (8-bit)
Length (16-bit)
Authenticator (48-bit for an accounting server, 64-bit for an
authentication server)
List of attributes
```

CLI configuration

To generate periodic accounting requests, set the Acct-Sess-Interval parameter in the External-Auth profile's Rad-Acct-Client subprofile.

VT100 configuration

To generate periodic accounting requests, set the Sess Timer parameter in the Ethernet > Mod Config > Accounting menu,

Example of classifying user sessions

Suppose that the TAOS unit has three classes of clients: Class-1, Class-2, and Class-3. At the time of the sessions report, there are eight active sessions: three Class-1 sessions, four Class-2 sessions, and one Class-3 session. The accounting packet that the TAOS unit sends to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of the class/session pairs.

Understanding RADIUS Authentication 2

Introduction 2-1
RADIUS profile formats 2-1
Pre-authentication 2-2
RADIUS password handling 2-3
Authenticating framed protocol sessions 2-5
Token-card authentication 2-8
Tunnel authentication 2-14
Callback after authentication 2-19

Introduction

Authentication is the first line of defense against unauthorized access to your network. It uses an exchange of information to verify the identity of a user. The information is usually encrypted at both ends. In determining which type of authentication to use, you should consider whether the call is between two machines or between a human being and a machine, and then decide how strong the authentication mechanism must be.

For example, if the connection is negotiated between two machines, you should consider whether the other location is trusted, whether that machine protects its own networks against security attacks, and whether it is physically accessible to many users. If the connection is negotiated with a user who must type in a token or password, you should consider how secure the password is and how frequently you want it to change. Once the user's connection is authenticated, you can use authorization restrictions to prevent the caller from accessing systems or networks you want to protect.

RADIUS profile formats

RADIUS user entries are composed of three parts:

```
User-Name Check-Items
       Reply-Items
```

Each element is described below.

- User-Name

The User-Name must be left justified. It is typically the name of the caller (or calling device), but it may also be a phone number, a special string indicating a pseudo-user profile, or the string DEFAULT (for the default user profile).

- Check-Items

  Check-Items must be on the same line as the User-Name, and must be separated by white space from the User-Name. For the user to be authenticated, Check-Items must include attribute-value pairs that match the attributes present in an Access-Request packet. Check-Items typically include the password for the entry.

- Reply-Items

  Reply-Items must be indented and separated from the User-Name and Check-Items by a newline. (If a Reply-Item is not indented, it is interpreted as the User-Name of a new entry.) Reply-Items includes zero or more attribute-value pairs returned in Access-Accept messages. These attribute-value pairs specify the services authorized for the user.

Pre-authentication

Calling Line ID (CLID) or Dialed Number Information Service (DNIS) verification occurs before the TAOS unit accepts a call and begins the process of authenticating a password.

- A CLID is the phone number of a calling device. You can use CLID for authentication only where the call information is available end-to-end and Automatic Number Identification (ANI) applies to the call. In some areas, the WAN provider might not be able to deliver CLIDs, or a caller might keep a CLID private. Typically, people use CLID to protect against a situation in which an unauthorized user obtains the name, password, and IP address of an authorized user, and calls in from another location.
- A DNIS number is the phone number the remote device calls to connect to the TAOS unit, but without a trunk group or dialing prefix specification. When the profile requires DNIS authentication, the number called must match a phone number in a local Connection profile or RADIUS user profile.

When a caller's profile specifies a CLID, the TAOS unit can compare that number to the one presented by the telco switch, and can therefore verify that the call is coming from a known location.

RADIUS uses the following attribute-value pairs for specifying CLID and DNIS numbers:

Attribute	Value
Calling-Station-Id (31)	Specifies the CLID—the phone number of the calling device. When a user dials in using MP or MP+, the calling device might have more than one phone number associated with it. In that case, the CLID is the phone number associated with the channel in use.
Called-Station-Id (30)	Specifies the DNIS number—the called-party number, an Information Element of the Q.931 ISDN signaling protocol.
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after called-number authentication. Valid values are Not-Require-Auth (0), which is the default, and Require-Auth (1).

For RADIUS-authenticated connections, if the Calling-Station-Id or Called-Station-Id value is known, it is included in the Access-Request to the RADIUS server. If the Calling-Station-Id is

specified on the first line of the profile, and the Calling-Station-Id presented to the server does not match the value of the Calling-Station-Id attribute, the Access-Request is rejected. The following user profile specifies a CLID:

```
emma User-Password="test", Calling-Station-Id="5551213"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Ascend-Assign-IP-Pool=1,
   Ascend-Route-IP=Route-IP-Yes
```

The user is limited to a specific phone number. This profile could be used to prevent multiple user connections. Unless the user owns a PBX or other service that always gives out the same number for multiple phone lines, only one user will be able to connect. CLID authentication is normally used for security—to prevent a system admin or other important account from be abused.

RADIUS password handling

RADIUS supports connection-specific passwords and reserved passwords. You can set up password aging and expiration, specify a default profile, and use shared secrets.

Reserved RADIUS passwords

In addition to the connection-specific password typically assigned to a specific user profile, the RADIUS recognizes the following reserved values for the User-Password (2) attribute:

Password values	Description
`UNIX`	Instructs the RADIUS server use UNIX authentication. This password does not work with the CHAP protocol.
`SAFEWORD`	Instructs the RADIUS server to request validation from an Enigma Logic SafeWord server. (For details, see “Token-card authentication” on page 2-8.)
`ACE`	Instructs the RADIUS server to request validation from a Security Dynamics ACE server. (For details, see “Token-card authentication” on page 2-8.)
`ascend`	Used for pseudo-user and other system profiles. When this password is in use, the Service-Type attribute should always specify Outbound-User. This setting prevents callers from accessing the network using a well-known password. *Although the system does not reject the profile without the Outbound-User setting, omitting it introduces a serious security risk.*
`Ascend-CLID` or `Ascend-DNIS`	Used for pre-authenticating calls using CLID or DNIS information When these passwords are in use, the Service-Type attribute should always specify Outbound-User. This setting prevent callers from accessing the network using a well-known password. *Although the system does not reject the profile without the Outbound-User setting, omitting it introduces a serious security risk.*

Password expiration

Some RADIUS daemons support password aging and expiration, and provide a method for enabling users who dial into the terminal server to replace expired passwords. Password expiration does not work for passwords that are not stored in the RADIUS database (UNIX-authenticated or token-card passwords), or reserved passwords (such as `ascend`).

The following attribute-value pairs support password aging and expiration.

Attribute	Value
Ascend-PW-Expiration (21)	Expiration date for the user's password (consisting of a month, day, and year specification.) Its value can be updated automatically when a user renews a password. You must specify Ascend-PW-Expiration as a Check-Item.
Ascend-PW-Lifetime (208)	Number of days a password can be valid. You can specify an integer from 0 (the default) to 65535. The default disables password expiration. If the attribute is set to a nonzero value, and the user changes the password, the TAOS unit adds the value to the current date and updates the Ascend-PW-Expiration date. This method provides a way of specifying new expiration dates automatically rather than hard-coding a date.
Ascend-PW-Warntime (207)	Number of days a user will be warned that his or her password is about to expire (an integer from 0 to 65535).

Following is a portion of a sample profile for a user whose password expires on December 31, 1999:

```
brian User-Password="localpw", Ascend-PW-Expiration="Dec 31, 1999"
   Ascend-PW-Lifetime=30,
   Ascend-PW-Warntime=2,
   ...
```

When the user dials in on December 29, 1999, he receives a message that his password will expire in two days. If he changes the password at that time (by using the Password command in the terminal server), the RADIUS server updates the password, adds 30 days to the current date, and updates the Ascend-PW-Expiration date to January 30, 2000.

If the user dials in on December 31, 1999, he receives a message that his password has expired, and he is prompted to enter both the expired password and a new one. The system prompts twice for the new password to verify the entry. If the user enters the information incorrectly, the system displays another prompt and the user can try again, for a total of up to three attempts.

If the update is successful, the system sends the new password to the RADIUS server and displays the following message, immediately followed by the terminal-server prompt:

```
Password Updated
```

If the update fails for any reason, the following message appears:

```
Password NOT Changed
```

The DEFAULT user profile

A special user profile named DEFAULT can be placed at the end of the users file to specify what to do with users who do not have a profile. Only one DEFAULT entry is allowed, and it must be the last entry in the file. For example, the following entry allows terminal-server users to log in using their UNIX account names and passwords:

```
DEFAULT User-Password="UNIX"
   Service-Type=Login-User,
   Login-Service=Telnet
```

Shared secrets and secure exchanges

A shared secret is used to authenticate packets exchanged between the TAOS unit and the RADIUS server, and to encrypt passwords from dial-in callers before sending them across the local network. A shared secret is a single value known to both systems.

Figure 2-1 shows a basic example of how passwords presented by incoming calls are handled between the systems:

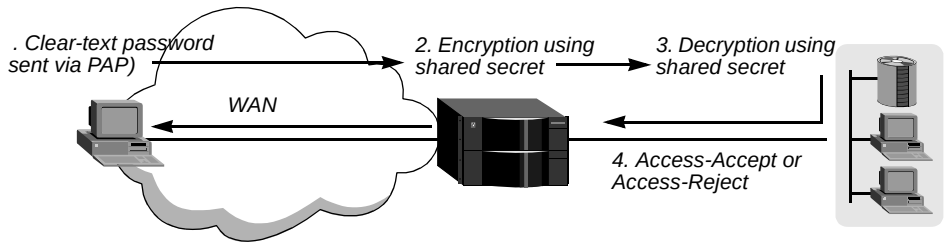


Figure 2-1. Shared secret used between the TAOS unit and a RADIUS server

The shared secret is used to encrypt the password from the dial-in call before sending it across the local network to a RADIUS server. The encryption makes use of the shared secret, the Authenticator field, and an encoding method, such as MD5, CHAP, or DES.

For dial-out calls, the RADIUS server sends the remote-end password to the Network Access Server (NAS). RADIUS encrypts passwords before sending them to the NAS if the dial-out profile uses the Ascend-Send-Secret (214) attribute to specify the password. If the profile specifies Ascend-Send-Secret and the RADIUS daemon does not encrypt the password, authentication will fail.

If the dial-out profile uses the Ascend-Send-Passwd (232) attribute to specify the password instead, the RADIUS daemon performs no encryption before sending the password to the NAS. This configuration may be required if you are using a RADIUS server that does not support outbound password encryption.

Unless you are using a RADIUS daemon that does not support Ascend-Send-Secret, its use is recommended in place of Ascend-Send-Passwd. Using Ascend-Send-Secret protects against local sniffers detecting dial-out passwords.

Authenticating framed protocol sessions

During establishment of a PPP data link, the dialing and answering units use Link Control Protocol (LCP) packets to negotiate the authentication protocol. After completing LCP

negotiations, the TAOS unit authenticates the user by means of the agreed-upon authentication protocol. It then negotiates the upper layer Network Control Protocols (NCPs) to set up the link's network-layer protocols.

If the link is configured to require authentication, the units at each end negotiate an authentication protocol. The answering unit always determines which authentication method to use for the call. A multilink connection begins with authentication of a base channel, and subsequent channels are authenticated separately when they are added to the call.

Specifying an authentication protocol required for dial-in calls

To require an authentication protocol for name and password authentication of framed sessions, you must configure the TAOS unit locally. You can specify any of the following protocols:

- Password Authentication Protocol (PAP), which provides a simple method for the TAOS unit to establish its identity in a two-way handshake. The remote device must support PAP.
- Challenge Handshake Authentication Protocol (CHAP), which is more secure than PAP. When the TAOS unit is using CHAP to authenticate the remote device, the system can periodically verify the identity of the remote device by means of a three-way handshake and encryption. The remote device must support CHAP.
- Microsoft CHAP (MS-CHAP), which uses DES and MD4 encryption. It is used primarily by Windows NT and LAN Manager systems.

How PAP works

PAP is a two-way handshake method of establishing a caller's identity. Used only once, during the initial establishment of the data link, PAP is not a strong authentication method. Passwords are sent as plain text across the WAN, so eavesdroppers with the proper equipment and software can potentially detect and reuse correct passwords.

PAP authentication is typically used because the available password method or database requires it. For example, if the UNIX password file is used to authenticate calls (by means of RADIUS), the TAOS unit forces the peer to use PAP.

When PAP is used with RADIUS authentication, the TAOS unit uses the shared secret to encrypt the text password it receives from the caller before sending the password across the network to the server. The RADIUS server decrypts the password using the same shared secret before performing authentication or passing it to another authentication server, such as a UNIX host or token-card server .

How CHAP and MS-CHAP work

CHAP authentication verifies the caller's identity by using a three-way handshake upon initial link establishment and possibly repeating the handshake any number of times. The authenticator sends a challenge to the caller. The caller responds with an MD5 digest calculated from the password. The authenticator then checks the digest against its own calculation of the expected hash value to authenticate the call. A new challenge can be sent at random intervals.

CHAP is a stronger authentication method than PAP, because the password is not sent as plain text. In addition, the use of repeated challenges limits the time of exposure to any single

attempt to break the encryption code, and the authenticator is in control of how often and when challenges are sent.

MS-CHAP is a close derivative of CHAP. However, CHAP is designed to authenticate WAN-aware secure software. It is not widely used to support remote workstations, where an insecure plain text login might be required. MS-CHAP addresses this issue, and also integrates the encryption and hashing algorithms used on Windows networks. Microsoft Windows NT and LAN Manager platforms implement MS-CHAP.

When CHAP or MS-CHAP is used with RADIUS authentication, the following events occur:

1. The TAOS unit sends a random, 128-bit challenge to the calling unit.
2. The calling unit calculates an MD5 digest by means of its password, the challenge, and the PPP packet ID.
3. The calling unit sends the MD5 digest, the challenge, and the PPP packet ID (but not the password) to the TAOS unit. The TAOS unit never has the caller's password.
4. The TAOS unit forwards the digest, along with the original challenge and PPP packet ID, to the RADIUS server. No encryption is necessary, because MD5 creates a one-way code that cannot be decoded.
5. The RADIUS server looks up the caller's password in a local database, and calculates an MD5 digest with the local version of the remote secret, along with the challenge and PPP packet ID received from the TAOS unit.
6. The RADIUS server compares the calculated MD5 digest with the digest it received from the TAOS unit. If the digests are the same, the passwords matched, and the call is accepted.

Requesting a protocol for use in dial-out calls

Dial-out RADIUS profiles can specify the authentication protocol and password used to send authentication information to the remote end. RADIUS uses the following attribute-value pairs to request an authentication protocol in a dial-out profile.

Attribute	Value
Ascend-Authen-Alias (203)	Login name for the TAOS unit to be sent as part of the authentication process of a dial-out call.
Ascend-Send-Auth (231)	Authentication protocol requested for a dial-out call. With the default Send-Auth-None (0) value, no authentication is negotiated. Other values are Send-Auth-PAP (1) and Send-Auth-CHAP (2).
Ascend-Send-Secret (214)	Password sent to the remote end during authentication of the dial-out call. If the server does not support this attribute, use Ascend-Send-Passwd (232) instead. For details, see "Shared secrets and secure exchanges" on page 2-5.

The following profiles request CHAP when the device dials out to the remote end:

```
hanif User-Password="localpw"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.1.2.3,
   Framed-IP-Netmask=255.255.255.248
```

```
route-tnt-1 User-Password="ascend", Service-Type=Outbound-User
   Framed-Route="10.1.2.3/29 10.1.2.3 1 n hanif-out"

hanif-out User-Password="localpw", Service-Type=Outbound-User
   User-Name="hanif",
   Ascend-Dial-Number="555-1212",
   Framed-Protocol=PPP,
   Framed-IP-Address=10.1.2.3
   Framed-IP-Netmask=255.255.255.248,
   Ascend-Send-Auth=Send-Auth-PAP,
   Ascend-Send-Secret="remotepw"
```

Token-card authentication

In token-card authentication, the RADIUS server is the intermediary between the TAOS unit answering the call and an External Authentication Server (EAS), such as a Security Dynamics ACE/Server or an Enigma Logic SafeWord server. In RADIUS, you can specify the following token-card authentication modes:

- PAP-TOKEN
- PAP-TOKEN-CHAP
- CACHE-TOKEN

Enhanced security with token cards

Token cards protect against both passive attacks and replay attacks. In a replay attack, an unauthorized user records valid authentication information exchanged between systems and then replays it later to gain entry. Because token cards provide one-time-only passwords, the password changes many times a day, making replay impossible.

Token cards are hardware devices, typically shaped liked credit-card calculators, with an LCD display that informs users about the current, one-time-only token (password) that will enable access to a secure network. The current token changes many times a day. Token cards keep the changing authentication information continuously up-to-date by maintaining a synchronized clock with an EAS such as an ACE/Server or SafeWord server. Authorized users must have the token card in their possession to gain access to a secure network.

If the EAS is ACE/Server, the user has a SecurID token card that displays a randomly generated access code, which changes every 60 seconds. If the EAS is SafeWord, the user can have one of the following types of token cards:

- ActivCard
- CryptoCard
- DES Gold
- DES Silver
- SafeWord SofToken
- SafeWord MultiSync
- DigiPass
- SecureNet Key

- WatchWord

The TAOS unit supports the use of token cards only through RADIUS. The RADIUS server must be configured to interact with the EAS modules, which typically run on the same physical system as the RADIUS server.

Note: When RADIUS authentication is in use, the RADIUS server itself acts as the EAS. When token-card authentication is in use, the RADIUS server passes the authentication request on to an ACE/Server or SafeWord server, and that system is referred to as the EAS. This does not affect the local profile configuration, which must still specify RADIUS as the external server.

A simple method of authenticating token-card calls

The TAOS unit can support token-card authentication from non-TAOS units by authenticating the calls in the terminal-server software. The unit uses normal PAP authentication to do the challenge-response token exchanges. For example, the following RADIUS profile specifies authentication from an ACE server:

```
carlos User-Password="ACE"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.2.3.78,
   Framed-IP-Netmask=255.255.255.255
```

The RADIUS server discards the user's response to the initial terminal-server Password prompt, so the user can enter any value. The RADIUS server generates an Access-Challenge with a challenge prompt (typically a Passcode prompt for ACE authentication), and uses the response to that challenge to actually authenticate the user with the EAS.

If the caller's profile specifies the following attribute-value pair, the system does not require a challenge-response exchange:

Attribute	Value
Ascend-Token-Immediate (200)	Bypasses the challenge-response procedure required by some token-card authentication methods. Valid values are Tok-Imm-No (0), which is the default, and Tok-Imm-Yes (1). If used, Ascend-Token-Immediate must be a Check-Item in the RADIUS profile. **Note:** Setting this attribute to Tok-Imm-Yes makes the profile incompatible with PAP-TOKEN, PAP-TOKEN-CHAP, and CACHE-TOKEN authentication.

When users have a token card that not require a challenge-response exchange (such as ACE), you can use Ascend-Token-Immediate to simplify the authentication process. Users respond to the initial Password prompt with the current token. The RADIUS server does not discard this initial response, but uses it to authenticate the call via the EAS.

Following is a sample RADIUS profile using Ascend-Token-Immediate:

```
robin User-Password="ACE", Ascend-Token-Immediate=Tok-Imm-Yes
   Service-Type=Framed-User,
```

```
Framed-Protocol=PPP,
Framed-IP-Address=10.3.4.5,
Framed-IP-Netmask=255.255.255.255
```

Authenticating token-card connections from TAOS units

Figure 2-2 shows a dial-in connection to a TAOS unit on a secure network. The remote user must use a token card to gain access to the secure network.

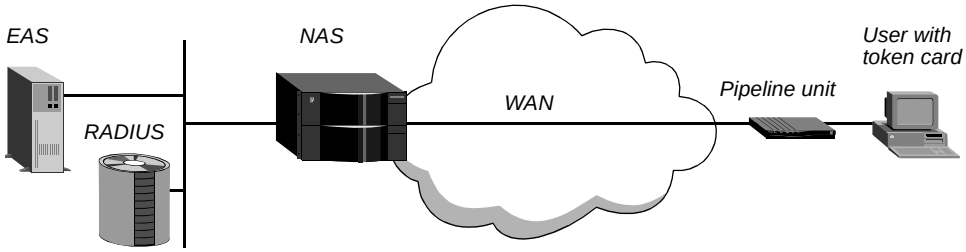


Figure 2-2. Token card authentication for dial-in connections

The following events take place:

1 A user with a token card initiates a connection to the TAOS unit (the NAS).

2 The NAS sends an Access-Request packet to the RADIUS server to authenticate the incoming call, and the RADIUS server forwards the connection request to the EAS (an ACE/Server or SafeWord server).

3 The EAS sends an Access-Challenge packet back through the RADIUS server and the TAOS unit to the user dialing in. The user sees the challenge message, obtains the current password from his or her token card, and enters that password in response to the challenge message. The password travels back through the NAS and the RADIUS server to the EAS.

4 The EAS sends a response to the RADIUS server, specifying whether the user has entered the proper token. If the user enters an incorrect token, the EAS returns another challenge and the user can try again, for a total of up to three attempts.

5 As the last step in authentication, the RADIUS server sends an authentication response to the TAOS unit. If authentication is unsuccessful, the TAOS unit receives an Access-Reject packet and terminates the call. If authentication is successful, the TAOS unit receives an Access-Accept packet containing a list of Attribute-Value pairs from the user profile in the RADIUS server's database. The TAOS unit uses the Attribute-Value pairs to create the connection.

Using PAP-TOKEN authentication

PAP-TOKEN is an extension of PAP authentication. It is not practical for multichannel calls, because if bandwidth requirements cause another channel to come up, the TAOS unit must interrupt the session to challenge the user for another token.

With PAP-TOKEN, the caller's send-password is sent as part of the initial session negotiation, which triggers a challenge from the EAS. The EAS returns a challenge, and the user types in the current token obtained from the token card. The token is sent in the clear (by means of PAP), but because it is used only once, sending the token in the clear may not considered a serious security risk. The response to the initial challenge authenticates the base channel of the

call. If bandwidth requirements cause another channel to come up, the user is challenged for a password.

Figure 2-3 shows a PC user with a SecurID token card dialing into the MAX TNT® unit through a Pipeline unit. The EAS is a UNIX host running RADIUS and Security Dynamics ACE software.

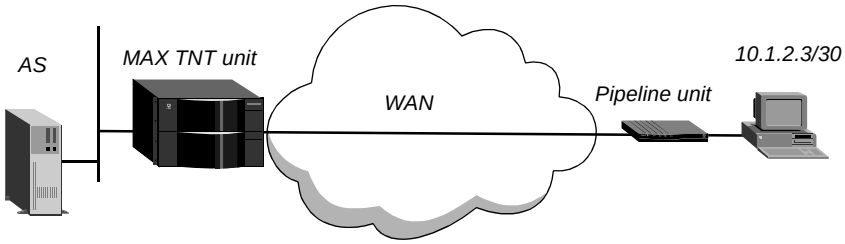


Figure 2-3. PAP-TOKEN with an ACE server

When the EAS sends an Access-Challenge packet back through the RADIUS server and the MAX TNT unit to the user dialing in, the user sees the challenge message, obtains the current token, and enters that password in response to the challenge message. The password travels back through the MAX TNT and the RADIUS server to the EAS, where it is authenticated. Following is a RADIUS profile for the PC user:

```
Connor User-Password="ACE"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.1.2.3,
   Framed-IP-Netmask=255.255.255.252
```

Using PAP-TOKEN-CHAP authentication

PAP-TOKEN-CHAP is appropriate for token-authenticating multilink calls. The base channel is authenticated by means of PAP-TOKEN. If channels are added to the call, they are authenticated by means of CHAP. When the initial call is authenticated, the RADIUS server informs the NAS of the password to expect for subsequent channels by sending the value as Ascend-Receive-Secret.

In addition to the requirement that the User-Password attribute must specify ACE or SAFEWORD, PAP-TOKEN-CHAP authentication requires the following attribute-value pair:

Attribute	Value
Ascend-Receive-Secret (215)	Text string of up to 20 characters, which must match the password sent by the remote end to authenticate added channels. The RADIUS server delivers the receive-secret to the NAS when the initial call is authenticated. The NAS stores the receive-secret for the caller, and uses it to create the digest sent to the RADIUS server by means of CHAP.

Figure 2-4 shows a user with a token card dialing into the MAX TNT unit through a Pipeline unit. The EAS is a UNIX host running RADIUS and Enigma Logic SafeWord server software. After authentication, the user can open a multilink session.

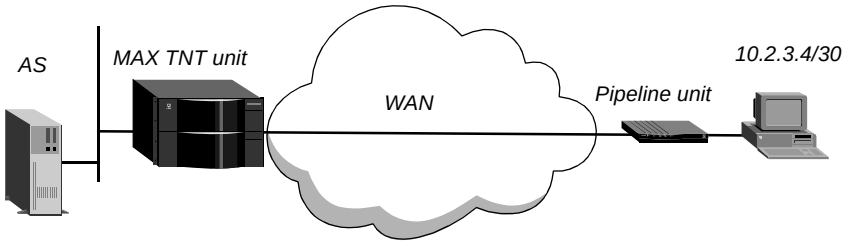


Figure 2-4. PAP-TOKEN-CHAP with a Safeword server

Following is a RADIUS user profile for the dial-in user:

```
Raoul User-Password="SAFEWORD"
   Service-Type=Framed-User,
   Framed-Protocol=MPP,
   Framed-IP-Address=10.2.3.4,
   Framed-IP-Netmask=255.255.255.252,
   Ascend-Receive-Secret="aux-send",
   Ascend-Base-Channel-Count=2,
   Ascend-Maximum-Channels=2
```

Using CACHE-TOKEN authentication

CACHE-TOKEN is another way of token-authenticating multilink calls. The RADIUS server caches an encrypted version of the token for a specified number of minutes. If the caller dials additional channels, the RADIUS server receives the request from the NAS, verifies that the token has not expired, and uses the cached token to authenticate the channels. If the token has expired, the request must be authenticated through the EAS with another challenge token.

In addition to the requirement that the User-Password attribute must specify ACE or SAFEWORD, CACHE-TOKEN authentication uses the following attribute-value pairs:

Attribute	**Value**
Ascend-Receive-Secret (215)	Text string of up to 20 characters, which must match the password sent by the remote end to authenticate the initial call. The RADIUS server uses this value to decrypt the hashed digest sent by the NAS. The hashed digest is derived from the token sent by the caller and the normal password in the remote-end profile.
Ascend-Token-Expiry (204)	Number of minutes a cached token remains valid. The default of 0 (zero) means that token caching is not allowed. Ascend-Token-Expiry must be a Check-Item. Token expiry is done solely in the RADIUS server. The NAS forwards authentication requests, and if the token has expired, the RADIUS server forwards the request to the EAS, which returns another challenge to the remote end.

Attribute	Value
Ascend-Token-Idle (199)	Number of minutes a cached token remains valid if a call is idle. By default, the token remains alive until the value of Ascend-Token-Expiry is reached. Ascend-Token-Idle must be a Check-Item. Ascend-Token-Idle is useful for enforcing authentication when a connection comes up again after an idle period. If you do not specify this attribute, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire. Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

Figure 2-5 shows a user who dials in using a Pipeline unit and is authenticated by an EAS, which is a UNIX host running RADIUS and Enigma Logic SafeWord server software.

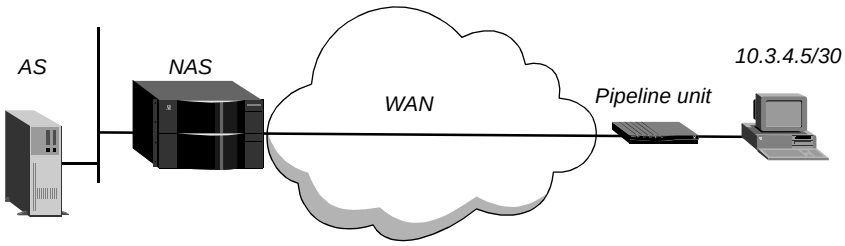


Figure 2-5. CACHE-TOKEN with a SafeWord server

Following is a RADIUS user profile for the dial-in user:

```
Aydin User-Password="SAFEWORD", Ascend-Token-Expiry=30,
Ascend-Token-Idle=10,
   Service-Type=Framed-User,
   Framed-Protocol=MPP,
   Framed-IP-Address=10.3.4.5,
   Framed-IP-Netmask=255.255.255.252,
   Ascend-Receive-Secret="chap-val",
   Ascend-Base-Channel-Count=2,
   Ascend-Maximum-Channels=2
```

Using ACE authentication for network users

If the EAS is a Secure Dynamics ACE server, multiple users on a remote network can dial in using a single profile that specifies the remote router name. To dial in, a user must enter the token in the following format:

```
token.username
```

The RADIUS server presents the *username* argument, rather than the name of the router, to the ACE server. Token caching still functions normally. All users share the same RADIUS profile, and RADIUS accounting uses the router name, not the real user name.

In Figure 2-6, multiple remote users are connected to a Pipeline unit named Alameda.

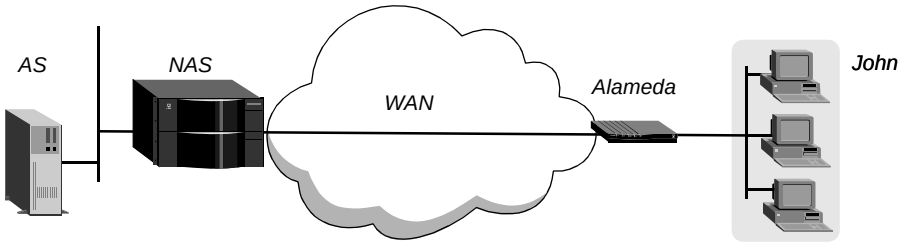


Figure 2-6. SACE authentication for remote router users

The following user profile specifies the system name of the Pipeline unit and the password for ACE authentication:

```
Alameda User-Password="ACE"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.72.138.1,
   Framed-IP-Netmask=255.255.255.0
```

A network user named John responds as follows to a password challenge:

```
From: hostname
0-Challenge: challenge
Enter next password: newtoken.John
```

Tunnel authentication

ATMP and L2TP support tunnel authentication. When tunnel authentication is required, the Foreign Agent (or L2TP Access Controller) initiating a tunnel request must supply a password before the Home Agent (or L2TP Network Server) allows registration of the tunnel.

Authenticating ATMP tunnels

The Home Agent ATMP profile specifies a password. If it is not null, Mobile Client profiles must supply the password to initiate a tunnel. If the Foreign Agent supplies the proper password when requesting a tunnel, the Home Agent returns a RegisterReply with a number that identifies the tunnel, and the Mobile Client's tunnel is established. If the password does not match, the Home Agent rejects the tunnel, and the Foreign Agent logs a message and disconnects the Mobile Client.

The Mobile Client's RADIUS profile must include the same value as the password specified in the local ATMP profile. In the following example, the password is `tunnel-password`:

```
mobile-client User-Password="my-password",
   Service-Type=Framed-User
   Tunnel-Type=ATMP,
   Tunnel-Server-Endpoint="3.3.3.3:8877",
   Tunnel-Password="tunnel-password"
```

If the profile specifies Tunnel-Password and the RADIUS daemon does not encrypt the password, tunnel authentication will fail. If the Mobile Client's profile uses the Ascend-Home-Agent-Password (184) attribute to specify the password instead, the RADIUS daemon performs no encryption before sending the password to the Home Agent. This

configuration might be required if you are using a RADIUS server that does not encrypt Tunnel-Password.

Note: Unless you are using a RADIUS daemon that does not support Tunnel-Password encryption (or encryption is not required), using the Tunnel-Password attribute is recommended, because it protects your system against local sniffers attempting to detect tunnel passwords.

Authenticating L2TP tunnels

L2TP tunnels can be authenticated using the same secret value in use at both ends of the connection (a shared secret). If Mobile Clients are authenticated by the LAC using RADIUS, the clients' RADIUS profiles can specify a shared secret by means of the Tunnel-Password (69) attribute.

Note: Tunnel-Password must be encrypted by the RADIUS daemon, or tunnel authentication will fail.

The following profile specifies the Tunnel-Password attribute:

```
l2tp-client User-Password="my-password"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.50.1.1,
   Framed-IP-Netmask=255.255.0.0,
   Tunnel-Type=L2TP,
   Tunnel-Medium-Type=IP,
   Tunnel-Server-Endpoint="lns-sys.domain.org"
   Tunnel-Password="tunnel-secret"
```

If you prefer, you can remove the Tunnel-Password attribute from calling clients' profiles and create a profile whose sole purpose is to authenticate L2TP tunnels. This configuration causes an extra RADIUS lookup the first time the tunnel is created, but it simplifies administration when shared secrets change. The RADIUS profile for tunnel authentication must specify the L2TP peer's name, a null password (""), and the Outbound-User setting for Service-Type. When an L2TP tunnel is initially established, both the LNS and the LAC issue a RADIUS lookup based on the peer's name. If the system finds a profile such as the following, it uses the Tunnel-Password value to authenticate the tunnel:

```
lns-sys.domain.org User-Password="", Service-Type=Outbound-User
   Tunnel-Password="tunnel-secret"
```

Note: The password in the pseudo-user profile must be null (""). Because this represents a security risk, *the profile must set the Outbound-User setting.*

Tunnel attribute sets with tags and preferences

The *RADIUS Attributes for Tunnel Protocol Support Internet-Draft* defines a set of RADIUS attributes designed to support transparent tunneling to dial-in networks, where a tunnel is created automatically without any explicit action by the user. To support this type of tunneling, the user's profile specifies a primary attribute set, which specifies all of the values required to set up the tunnel, as well as additional attribute sets that can be used to establish a tunnel if the primary server is unavailable.

Note: Use of tunneling attribute tags and preferences requires a RADIUS server that supports them. NavisRadius is one such server.

Overview of attribute sets and tags

A *tag* is a number from 1 to 31 that you can add to one or more of the RADIUS attributes listed in "Tunnel attributes used with tags" on page 2-17. Attributes that share the same tag number form an attribute set. Attribute sets in the same user profile are processed in numeric order (the set with tag 1 is processed before the set with tag 2, and so forth), unless the sets are reordered by means of the Tunnel-Preference attribute.

A tag value of 0 (zero) is considered untagged. Untagged attribute sets are processed before tagged attribute sets, unless a Tunnel-Preference setting specifies otherwise.

A tag is separated from an attribute-value pair by a colon. Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3:

```
joe User-Password="murphy"
    Tunnel-Type=L2TP : 1,
    Tunnel-Server-Endpoint="1.1.1.1" : 1,
    Tunnel-Password="loloaqic" : 1,
    Tunnel-Type=L2TP : 3,
    Tunnel-Server-Endpoint="3.3.3.3" : 3,
    Tunnel-Password="i82qb4ip" : 3,
    Tunnel-Type=L2F : 2,
    Tunnel-Server-Endpoint="2.2.2.2" : 2
    Tunnel-Password="itsAsecret" : 2
```

This profile specifies that the NAS (the TAOS unit) should attempt first to establish an L2TP tunnel to the LNS at 1.1.1.1. If that attempt fails, the system should attempt to bring up an L2F tunnel to a server at 2.2.2.2. If that attempt also fails, the system should try an L2TP tunnel to 3.3.3.3.

In this release, a user profile can specify up to 32 tunnel attribute sets. However, for each attempt to initiate a tunnel, the system waits for a certain interval before retrying, and retries a certain number of times (for example, as configured in the L2-Tunnel-Global profile). So, in practice, the client's PPP connection would typically time out long before 32 tunnel attempts were actually made.

Supported tunnel protocols

In this release, RADIUS attribute tags can be used for all supported tunnel protocols. The number of attribute sets used is limited for some protocols, as shown in the following table:

Tunnel protocol	Attribute sets used
L2TP	All specified attribute sets are used.
L2F	All specified attribute sets are used.
PPTP	Only the attribute set with the highest priority is used. Priority is defined by the Tunnel-Preference (83) value or by tag order.

Tunnel protocol	Attribute sets used
ATMP	Only the two sets with the highest priority are used. (From the second attribute set, only the Tunnel-Server-Endpoint (67) value is used. Other values can be omitted.) Priority is defined by the Tunnel-Preference (83) value or by tag order.

In the case of L2TP and L2F, you can use the DNS list attempt feature in conjunction with the tagging feature.

All the attribute sets in a profile must specify similar tunnel protocols, either all layer 3 tunnels (such as ATMP) or layer 2 tunnels (such as L2TP or L2F). You can mix L2TP and L2F, but not with ATMP. The following examples show two valid cases:

```
JL2 User-Password="example"
   Tunnel-Type=L2TP :1,
   Tunnel-Server-Endpoint=LNS-a.example.com :1,
   Tunnel-Type=L2F :2,
   Tunnel-Server-Endpoint=L2FGW.example.com :2
UL3 User-Password="example"
   Tunnel-Type=ATMP :1,
   Tunnel-Server-Endpoint=HA-a.example.com :1,
   Tunnel-Server-Endpoint=HA-b.example.com :2,
   Tunnel-Password=HApassword :1,
   Tunnel-Private-Group-ID=MyHomeNet :1
```

Tunnel attributes used with tags

Following are the relevant tunnel attribute-value pairs:

RADIUS attribute	Value
Tunnel-Type (64)	Tunneling protocol(s) to be used. In this release, only L2TP (3) and L2F (2) currently operate with full tunnel attribute and tag support.
Tunnel-Medium-Type (65)	Medium for establishing the tunnel. Currently, IP (1) is the only supported value.
Tunnel-Server-Endpoint (67)	IP address or hostname of the tunnel endpoint. If a DNS lookup returns several IP addresses, the system attempts to establish a tunnel to each address in turn.
Tunnel-Password (69)	Shared secret for authenticating the tunnel.

RADIUS attribute	Value
Tunnel-Preference (83)	Numeric preference value for an attribute set. If more than one set of tunneling attributes is returned by the RADIUS server to the TAOS unit, the Tunnel-Preference attribute can be included in a set to indicate its relative preference, with the lowest preference value designating the most preferred set. If no Tunnel-Preference is included in any of the attribute sets, the sets will be processed in the order of their respective tag numbers. If some but not all attribute sets contain a Tunnel-Preference value, the attribute sets without a Tunnel-Preference are designated as the least preferred sets. Attribute sets with identical preferences are processed in random order.
Tunnel-Client-Auth-ID (90)	Name of the Layer 2 Forwarding (L2F) tunnel initiator. This value is sent to the tunnel endpoint during tunnel authentication.
Ascend-Tunnel-VRouter-Name (31)	Name of a virtual router to use for establishing the L2TP or L2F tunnel. The specified VRouter must exist on the LAC.
Tunnel-Private-Group-ID (81)	Name of the Connection profile that defines the link on which the ATMP Home Agent transmits packets it receives from the Mobile Client. This attribute is supported only for ATMP tunnels. The value is used only if the Home Agent is in gateway mode. See Ascend-Home-Network-Name (185) for an alternate.

The TAOS unit currently ignores the following attributes if it receives them in a RADIUS response:

- Tunnel-Assignment-ID (82)
- Tunnel-Client-Endpoint (66)

Example of reordering sets using Tunnel-Preference

Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3, with a Tunnel-Preference value that changes the order in which the tunnels are attempted:

```
joe User-Password="murphy"
    Tunnel-Type=L2TP : 1,
    Tunnel-Server-Endpoint="1.1.1.1" : 1,
    Tunnel-Password="loloaqic" : 1,
    Tunnel-Type=L2TP : 3,
    Tunnel-Server-Endpoint="3.3.3.3" : 3,
    Tunnel-Password="i82qb4ip" : 3,
    Tunnel-Type=L2F : 2,
    Tunnel-Server-Endpoint="2.2.2.2" : 2
    Tunnel-Password="itsAsecret" : 2,
    Tunnel-Preference=100 : 2,
    Tunnel-Preference=200 : 1
```

With these preference values, the NAS makes the attribute set tagged 2 the primary attribute set, and first attempts to establish an L2F tunnel to a server at 2.2.2.2. It tries an L2TP tunnel to

the LNS at 1.1.1.1 only if the initial tunnel attempt fails. If that attempt also fails, the system attempts to establish an L2TP tunnel to 3.3.3.3.

Callback after authentication

Organizations use callback for a variety of reasons, such as saving on phone charges, but the primary use is for security. Using callback ensures that the connection is made with a known phone number. Hanging up and calling back adds a level of certainty that the connection is with a trusted user, especially because the TAOS unit calls back the user immediately after authentication (or CLID pre-authentication).

Because the connection is initiated by the caller, the system does not need an explicit dial-out profile or a method of locating the dial-out profile (such as an IP route). All the necessary information for dialing back to the caller is present in the user profile. The following attributes must be specified for callback:

Attribute	Value
Ascend-Callback (246)	Enables/disables callback. Callback-No (0) is the default. The other value is Callback-Yes (1).
Ascend-Dial-Number (227)	Phone number the TAOS unit dials to reach the remote end.
Ascend-Send-Secret (214)	Password sent to the remote end for authenticating a dial-out call. If the RADIUS server does not support Ascend-Send-Secret, use Ascend-Send-Passwd (232). For details, see “Shared secrets and secure exchanges” on page 2-5.

The RADIUS profile specifies pre-authentication using CLID and callback to the remote end:

```
5105551234 User-Password="Ascend-CLID"
   User-Name="clara-w95",
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.10.11.12,
   Ascend-Dial-Number="95551212",
   Ascend-Send-Auth=Send-Auth-PAP,
   Ascend-Send-Secret="test",
   Ascend-Callback=Callback-Yes
```

The following RADIUS profile specifies PPP authentication and callback to the remote end:

```
clara-w95 User-Password="test"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.10.11.12,
   Ascend-Dial-Number="95551212",
   Ascend-Send-Auth=Send-Auth-PAP,
   Ascend-Send-Secret="test",
   Ascend-Callback=Callback-Yes
```

Understanding RADIUS Accounting 3

What is RADIUS accounting? 3-1

What kinds of packets does RADIUS accounting use? 3-1

Proxy RADIUS accounting 3-11

Sample accounting records 3-13

What is RADIUS accounting?

RADIUS accounting records information about WAN sessions only. Specifically, RADIUS logs information about three types of events:

- Start session. Denotes the beginning of a session with the TAOS unit. Information about this event appears in an accounting Start record.
- Stop session. Denotes the end of a session with the TAOS unit. Information about this event appears in an accounting Stop record.
- Failure-to-start session. Denotes that a login attempt has failed. Information about this event appears in an accounting Failure-to-start record.

When the TAOS unit recognizes one of these events, it sends an accounting request to RADIUS. When the accounting server receives the request, it combines the information into a record and timestamps it. Each type of accounting record contains attributes associated with an event type, and can show the number of packets the TAOS unit transmitted and received, the protocol in use, the user name and IP address of the client, and other information about the connection. All counters are session based, and reset to 0 (zero) when the session starts. At the end of the session, the interfaces are reported as Down and show 0 (zero).

You can use RADIUS accounting to:

- Gather billing information, including who called, how long the session lasted, and how much traffic occurred during the session.
- Troubleshoot RADIUS and TAOS operations. Accounting records can contain information about how many login failures occurred, and can describe the characteristics of the failed attempts.

What kinds of packets does RADIUS accounting use?

RADIUS accounting uses two kinds of packets: Accounting Start and Accounting Stop.

Accounting Start packets

Accounting Start packets signal a Start session event. When a terminal-server call passes authentication, or the user logs in for a routing session, the TAOS unit sends an Accounting Start packet to the RADIUS accounting server. The packet describes the type of session in use and the name of the user opening the session.

The TAOS unit does not send an Accounting Start packet if a call fails authentication or otherwise fails to log in. In some cases, a session begins with a user login and then authentication follows, such as when a terminal-server user chooses PPP or SLIP after login. If Service-Type=Login-User, or if Service-Type is unspecified, the TAOS unit sends an Accounting Start packet after login. Information from an Accounting Start packet appears in a Start record.

Accounting Stop packets

Accounting Stop packets signal a Stop session or Failure-to-start session event. By default, the TAOS unit always sends an Accounting Stop packet at the end of a session, including cases in which a user fails authentication. Information from an Accounting Stop packet appears in a Stop record or Failure-to-start record.

RADIUS attributes in Start records

Table 3-1 lists the RADIUS attributes that can appear in a Start record.

Table 3-1. RADIUS attributes in Start records

Attribute	Description
Acct-Authentic (45)	Indicates the method the TAOS unit used to authenticate an incoming call: • RADIUS (1) indicates that RADIUS authenticated the incoming call. • Local (2) indicates that the TAOS unit used a local Connection profile, TACACS profile, or TACACS+ profile, or that the TAOS unit accepted the call without authentication.
Acct-Delay-Time (41)	Indicates the number of seconds the TAOS unit has been trying to send the Accounting packet. In an Accounting Start packet, this value is 0 (zero).
Acct-Session-Id (44)	Consists of a unique numeric string identified with the routing or terminal-server session reported in the Accounting packet. The string is a random number. RADIUS correlates the Accounting Start packet and Accounting Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.

Table 3-1. RADIUS attributes in Start records (continued)

Attribute	Description
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are Accounting Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type=Stop are Accounting Stop packets. The information in these packets appears in Stop or Failure-to-start records.
Ascend-Calling-Subaddress (107)	Specifies the ISDN subaddress that the TAOS unit sends to RADIUS during CLID authentication.
Ascend-Dial-Number (227)	Indicates the phone number of the device that originated the connection.
Ascend-Modem-PortNo (120)	Specifies the number of the port on the specified slot that terminates the call.
Ascend-Modem-ShelfNo (122)	Specifies the number of the shelf that terminates the call.
Ascend-Modem-SlotNo (121)	Specifies the number of the slot on the specified shelf that terminates the call.
Ascend-Owner-IP-Addr (86)	Specifies the IP address of the owner of the Multilink bundle.
Ascend-Redirect-Number (109)	Indicates the redirected number extracted from the Redirect Number Information Element (IE) in an ISDN frame.
Ascend-Session-Svr-Key (151)	Identifies the user session in which a client sends a disconnect or filter-change request to the RADIUS server.
Ascend-User-Acct-Base (142)	Indicates whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.
Ascend-User-Acct-Host (139)	Indicates the IP address of the RADIUS server to use for the link.
Ascend-User-Acct-Key (141)	Indicates the RADIUS client password.
Ascend-User-Acct-Port (140)	Indicates a destination UDP port number for the connection.
Ascend-User-Acct-Time (143)	Indicates the number of seconds the TAOS unit waits for a response to a RADIUS accounting request.
Ascend-User-Acct-Type (138)	Indicates the RADIUS accounting server(s) to use for the connection.
Called-Station-Id (30)	Indicates the called-party number, which is the phone number the user dials to connect to the TAOS unit.

Table 3-1. RADIUS attributes in Start records (continued)

Attribute	Description
Calling-Station-Id (31)	Indicates the calling-party number, which is the phone number of the user that has connected to the unit.
Class (25)	Enables access providers to classify their user sessions. The default value for the Class attribute is null.
Framed-IP-Address (8)	Indicates the IP address of the user starting the session. The default value is 0.0.0.0.
Framed-Protocol (7)	Indicates the kind of protocol the connection uses.
NAS-IP-Address (4)	Indicates the IP address of the TAOS unit.
NAS-Port (5)	Indicates the port on which the TAOS unit received the call.
NAS-Port-Type (61)	Specifies the type of service in use for the established session: • NAS_Port_Type_Async (0) indicates a call the TAOS unit routes to a digital modem. • NAS_Port_Type_Sync (1) indicates a synchronous ISDN connection.
User-Name (1)	Indicates the name of the user starting the session.

RADIUS attributes in Stop records

Table 3-2 lists the RADIUS attributes that can appear in a Stop record.

Table 3-2. RADIUS attributes in Stop records

Attribute	Description	Conditions for inclusion
Acct-Authentic (45)	Indicates the method the TAOS unit used to authenticate an incoming call: • RADIUS (1) indicates that RADIUS authenticated the incoming call. • Local (2) indicates that the TAOS unit used a local Connection profile, TACACS profile, or TACACS+ profile, or that the TAOS unit accepted the call without authentication.	Session must be authenticated.

Table 3-2. RADIUS attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Delay-Time (41)	Indicates the number of seconds between the time an event occurred and the time the TAOS unit sent the packet. If RADIUS does not acknowledge the packet, the TAOS unit resends it. The value of Acct-Delay-Time changes to reflect the proper event time.	None.
Acct-Input-Octets (42)	Indicates the number of octets the TAOS unit received during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Acct-Input-Packets (47)	Indicates the number of packets the TAOS unit received during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated. A framed protocol must be in use.
Acct-Link-Count (51)	Indicates the highest number of channels connected.	Session must be authenticated.
Acct-Multi-Session-Id (50)	Reports the ID number of the Multilink bundle when the session closes.	Session must be authenticated.
Acct-Output-Octets (43)	Indicates the number of octets the TAOS unit sent during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Acct-Output-Packets (48)	Indicates the number of packets the TAOS unit sent during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated. A framed protocol must be in use.

Table 3-2. RADIUS attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Session-Id (44)	Consists of a unique numeric string identified with the routing or terminal-server session reported in the Accounting packet. The string is a random number of up to seven digits. RADIUS correlates the Accounting Start packet and Accounting Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.	None.
Acct-Session-Time (46)	Indicates the number of seconds the session has been logged in.	Session must be authenticated.
Acct-Status-Type (40)	Requests that have Acct-Status-Type set to Start are Accounting Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type set to Stop are Accounting Stop packets. The information in these packets appears in Stop or Failure-to-start records.	None.
Ascend-Calling-Subaddress (107)	Specifies the ISDN subaddress that the TAOS unit sends to RADIUS during CLID authentication.	None.
Ascend-Connect-Progress (196)	Indicates the state of the connection before it disconnects.	None.
Ascend-Data-Rate (197)	Indicates the rate of data received on the connection in bits per second.	None.
Ascend-Dial-Number (227)	Indicates the phone number of the device that originated the connection.	None.
Ascend-Disconnect-Cause (195)	Indicates the reason a connection was taken offline.	None.
Ascend-Event-Type (150)	Indicates a cold-start notification, informing the accounting server that the TAOS unit has started up.	For a cold-start notification, the TAOS unit sends values for NAS-IP-Address and Ascend-Event-Type in an Ascend-Access-Event-Request packet (code 33). The RADIUS accounting server must send an Ascend-Access-Event-Response packet (code 34), with the correct identifier, to the TAOS unit.

Table 3-2. RADIUS attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-First-Dest (189)	Records the destination IP address of the first packet the TAOS unit received on a connection after authentication.	Session must be authenticated.
Ascend-Home-Agent-IP-Addr (183)	Indicates the IP address of the Home Agent associated with the Mobile Client.	Session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).
Ascend-Home-Agent-UDP-Port (186)	Indicates the UDP port number to use when the Foreign Agent sends ATMP packets to the Home Agent.	Session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).
Ascend-Home-Network-Name (185)—Gateway mode only	Indicates the name of the Connection profile through which the Home Agent sends all packets it receives from the Mobile Client during ATMP operation.	Session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).
Ascend-Modem-PortNo (120)	Specifies the number of the port on the specified slot that terminates the call.	None.
Ascend-Modem-ShelfNo (122)	Specifies the number of the shelf that terminates the call.	None.
Ascend-Modem-SlotNo (121)	Specifies the number of the slot on the specified shelf that terminates the call.	None.
Ascend-Multilink-ID (187)	Reports the ID number of the Multilink bundle when the session closes.	Session must be authenticated.
Ascend-Num-In-Multilink (188)	Records the number of sessions remaining in a Multilink bundle when the session closes.	Session must be authenticated.
Ascend-Number-Sessions (202)	Indicates the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.	The TAOS unit sends Ascend-Number-Sessions in Ascend-Access-Event-Request packets. Only RADIUS daemons you customize to recognize packet code 33 respond to these request packets.
Ascend-Owner-IP-Addr (86)	Specifies the IP address of the owner of the Multilink bundle.	Session must be authenticated.

Table 3-2. RADIUS attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Pre-Input-Octets (190)	Reports the number of octets the TAOS unit received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Ascend-Pre-Input-Packets (192)	Reports the number of packets the TAOS unit received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated.
Ascend-Pre-Output-Octets (191)	Reports the number of octets the TAOS unit sent before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Ascend-Pre-Output-Packets (193)	Reports the number of packets the TAOS unit sent before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated.
Ascend-PreSession-Time (198)	Indicates the length of time, in seconds, from when a call connected to when it completed authentication.	None.
Ascend-Redirect-Number (109)	Indicates the redirected number extracted from the Redirect Number Information Element (IE) in an ISDN frame.	None.
Ascend-User-Acct-Base (142)	Indicates whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.	None.
Ascend-User-Acct-Host (139)	Indicates the IP address of the RADIUS server to use for the connection.	None.
Ascend-User-Acct-Key (141)	Indicates the RADIUS client password.	None.

Table 3-2. RADIUS attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-User-Acct-Port (140)	Indicates a destination UDP port number for the connection.	None.
Ascend-User-Acct-Time (143)	Indicates the number of seconds the TAOS unit waits for a response to a RADIUS accounting request.	None.
Ascend-User-Acct-Type (138)	Indicates the RADIUS accounting server(s) to use for the connection.	None.
Ascend-Xmit-Rate (255)	Indicates the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial connection.	None.
Called-Station-Id (30)	Indicates the called-party number, which is the phone number the user dials to connect to the TAOS unit.	None.
Calling-Station-Id (31)	Indicates the calling-party number, which is the phone number of the user that has connected to the unit.	None.
Class (25)	Enables access providers to classify their user sessions. The default value for the Class attribute is null.	None.
Framed-IP-Address (8)	Indicates the IP address of the user starting the session. The default value is 0.0.0.0.	None.
Framed-Protocol (7)	Indicates the kind of protocol the connection uses.	None.
NAS-IP-Address (4)	Indicates the IP address of the TAOS unit. This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.	None.
NAS-Port (5)	Indicates the port on which the TAOS unit received the call. NAS-Port does not appear in an Accounting-Stop packet for a Failure-start-session event.	None.

Table 3-2. RADIUS attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
NAS-Port-Type (61)	Specifies the type of service in use for the established session: NAS_Port_Type_Async (0) indicates a call the TAOS unit routes to a digital modem. NAS_Port_Type_Sync (1) indicates a synchronous ISDN connection.	None.
User-Name (1)	Indicates the name of the user starting the session.	None.
Tunnel-Client-Endpoint (66)	Specifies a string assigned by RADIUS that specifies the name for the unit placing the call.	None.
Tunnel-ID (68)	Specifies a string assigned by RADIUS to each session using CLID or DNIS tunneling.	None.
Tunnel-Type (64)	Specifies whether a session used the ATMP tunneling protocol.	None.

RADIUS attributes in Failure-to-start records

Failure-to-start records can contain only a subset of the information found in Stop records. The following attributes can appear:

Acct-Delay-Time (41)
Acct-Session-Id (44)
Acct-Status-Type (40)
Ascend-Connect-Progress (196)
Ascend-Data-Rate (197)
Ascend-Disconnect-Cause (195)
Ascend-PreSession-Time (198)
NAS-IP-Address (4)

For a brief description of each of these attributes, see Table 3-2 on page 3-4.

Proxy RADIUS accounting

The master shelf controller keeps track of all accounting Start records sent by host cards. If the shelf controller determines that a host card has gone down for any reason, it acts as proxy for the card and sends the accounting server a fail-safe Stop record for each of the card's open sessions. The host card might be brought down administratively, might be removed from the system, or might go down due to an error condition.

How proxy RADIUS accounting works

In general, when RADIUS accounting is in use, the situation shown in Figure 3-1 occurs.

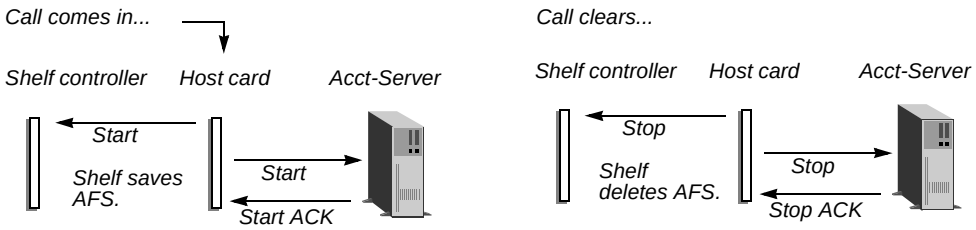


Figure 3-1. Normal RADIUS accounting (no proxy necessary)

When a call comes in, the host card first sends a Start record to the shelf controller, which stores it as an Accounting Fail-Safe (AFS) record. The host card then sends one or more Start records to the RADIUS accounting server, repeating until it receives an ACK from the server. Similarly, when the call clears, the host card sends a Stop record to the shelf controller, which causes it to delete the AFS record for that session. The host card then sends the accounting server Stop records until it receives an ACK from the server.

When RADIUS accounting is in use and the host card goes down for any reason, proxy accounting occurs, as shown in Figure 3-2.

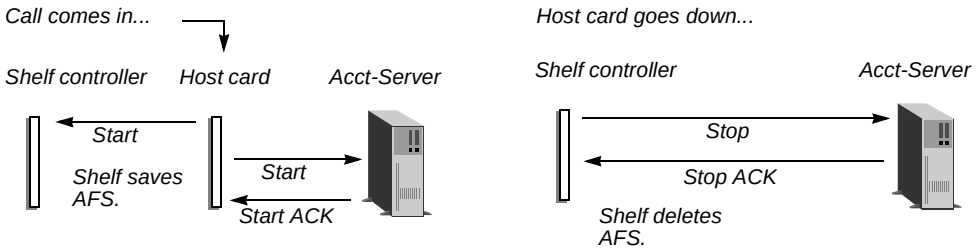


Figure 3-2. Proxy accounting (host card goes down)

In this case, when the shelf controller notes that the host card is down, it uses its own information about the host card and the stored AFS record to send a Stop record directly to the RADIUS accounting server, repeating until it receives a Stop ACK from the server. The shelf controller then deletes the AFS record for that session. However, if the accounting server is accessible only by means of the host card that goes down, Stop records cannot be delivered successfully.

Contents of the Stop record sent by proxy

The AFS Stop record does not contain all the information that appears in a record sent by a host card. In particular, it does not contain the input/output octet count fields or any other dynamic information related to the session. In Table 3-3, Yes indicates that the attribute is included in the Stop record. No indicates that the attribute is not included in the record or is set to null.

Table 3-3. RADIUS attributes included in proxy Stop records

Attribute in regular Stop record	In proxy Stop record
Acct-Authentic	Yes
Acct-Delay-Time	Yes
Acct-Input-Octets	No
Acct-Input-Packets	No
Acct-Multi-Session-Id	Yes
Acct-Output-Octets	No
Acct-Output-Packets	No
Acct-Session-Id	Yes
Acct-Status-Type	Yes
Acct-Session-Time	Yes. (The session time is accurate to within a few seconds.)
Ascend-Connect-Progress	Yes
Ascend-Data-Rate	Yes
Ascend-Disconnect-Cause	Yes. (The Disconnect reason is always 210, slot card down.)
Ascend-First-Dest	No
Ascend-Home-Agent-IP-Addr	Yes
Ascend-Home-Agent-UDP-Port	Yes
Ascend-Multilink-ID	Yes
Ascend-Num-In-Multilink	Yes
Ascend-Owner-IP-Addr	Yes
Ascend-Pre-Input-Octets	No
Ascend-Pre-Input-Packets	No

Table 3-3. RADIUS attributes included in proxy Stop records (continued)

Attribute in regular Stop record	In proxy Stop record
Ascend-Pre-Output-Octets	No
Ascend-Pre-Output-Packets	No
Ascend-PreSession-Time	Yes
Calling-Station-Id	No
Class	Yes
Framed-IP-Address	Yes
Framed-Protocol	Yes
Login-IP-Host	Yes
Login-Service	Yes
Login-TCP-Port	Yes
NAS-IP-Address	Yes
NAS-Port	Yes
NAS-Port-Type	Yes
Tunnel-Type	Yes
User-Name	Yes

Sample accounting records

This section provides sample Start and Stop records for the following configurations:

- A Pipeline unit dialing into a MAX TNT unit
- A modem calling into a MAX™ unit
- An immediate-modem dialout connection

The section also illustrates a Stop record sent by proxy.

A Pipeline unit dialing into a MAX TNT unit

When a Pipeline unit dials into a MAX TNT unit, the Start record might look like the following:

```
Tue Feb 18 12:00:41 1999 /* Session startup time */
   User-Name="ht-net" /* The name of the Pipeline unit */
   NAS-IP-Address=206.65.212.46 /* The IP address of the MAX TNT unit*/
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Start /* Start record. */
   Acct-Delay-Time=0 /* Always zero for a Start record */
   Acct-Session-Id="1234567" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication in use */
   Called-Station-Id="3142" /* Called-party number */
   Framed-Protocol=PPP /* PPP call */
   Framed-IP-Address=11.0.0.1 /* IP address of the Pipeline unit */
```

The Stop record might look like the following:

```
Tue Feb 18 12:02:48 1999 /* Session hangup time */
   User-Name="ht-net" /* The name of the Pipeline unit */
   NAS-IP-Address=206.65.212.46 /* The IP address of the MAX TNT unit*/
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Ascend-Owner-IP-Addr=206.65.212.46 /* Owner of Multilink bundle */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* Unit tried to send packet for 18 seconds */
   Acct-Session-Id="1234567" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication used */
   Acct-Session-Time=128 /* Number of seconds in session */
   Acct-Input-Octets=2421 /* Bytes received from the Pipeline unit */
   Acct-Output-Octets=1517 /* Bytes sent to the Pipeline unit */
   Acct-Input-Packets=79 /* Packets received from the Pipeline unit */
   Acct-Output-Packets=47 /* Packets sent to the Pipeline unit */
   Ascend-Disconnect-Cause=100 /* Session timeout */
   Ascend-Connect-Progress=60 /* LAN session up */
   Ascend-Data-Rate=31200 /* Receive data rate in bits per second */
   Ascend-Xmit-Rate=48000 /* Transmit data rate in bits per seconds */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-Packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-Packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle */.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Called-Station-Id="3142" /* Called-party number */
   Framed-Protocol=PPP /* PPP call */
   Framed-IP-Address=11.0.0.1 /* IP address of the Pipeline unit */
```

A modem calling into a MAX unit

If a modem dials into a MAX unit to reach its terminal server, the call can only be an unframed call. It cannot be a PPP, MP, or MP+ call. Therefore, the attributes Framed-Protocol and Framed-IP-Address do not appear in the sample records, and Login-Service=Unframed-User.

A Start record might look like the following:

```
Tue Feb 18 12:00:00 1999 /* Session startup time */
   User-Name="Berkeley" /* The name of the modem caller */
   NAS-IP-Address=200.65.212.46 /* The IP address of the MAX unit */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Start /* Start record. */
   Acct-Delay-Time=0 /* Always zero for a Start record */
   Acct-Session-Id="3456789" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication in use */
   Called-Station-Id="3143" /* Called-party number */
   Login-Service=Unframed-User /* Modem call */
```

The Stop record might look like the following:

```
Tue Feb 18 12:03:00 1999 /* Session hangup time */
   User-Name="Berkeley" /* The name of the modem caller */
   NAS-IP-Address=200.65.212.46 /* The IP address of the MAX unit */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Ascend-Owner-IP-Addr=206.65.212.46 /* Owner of Multilink bundle */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* Unit tried to send packet for 18 seconds */
   Acct-Session-Id="3456789" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication used */
   Acct-Session-Time=128 /* Number of seconds in session */
   Acct-Input-Octets=2421 /* Bytes received from the Pipeline unit*/
   Acct-Output-Octets=1517 /* Bytes sent to the Pipeline unit */
   Acct-Input-Packets=79 /* Packets received from the Pipeline unit */
   Acct-Output-Packets=47 /* Packets sent to the Pipeline unit */
   Ascend-Disconnect-Cause=100 /* Session timeout */
   Ascend-Connect-Progress=60 /* LAN session up */
   Ascend-Data-Rate=31200 /* Receive data rate in bits per second */
   Ascend-Xmit-Rate=48000 /* Transmit data rate in bits per seconds */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-Packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-Packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle *.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Called-Station-Id="3143" /* Called-party number */
   Login-Service=Unframed-User /* Modem call */
```

An immediate-modem dialout connection

An accounting start/stop pair is generated whenever an immediate-modem dialout connection is initiated or dropped. The accounting start/stop records generated by a call include the Calling-Station-Id attribute to indicate the called number, as shown in the following sample records:

```
Fri May 1 11:08:04 1998
   User-Name="kevtest"
   NAS-IP-Address=10.11.21.30
   NAS-Port=0
   NAS-Port-Type=Sync
   Acct-Status-Type=Start
   Acct-Delay-Time=0
   Acct-Session-Id="262862705"
   Acct-Authentic=Local
   Calling-Station-Id="8005"

Fri May 1 11:08:33 1998
   User-Name="kevtest"
   NAS-IP-Address=10.11.21.30
   NAS-Port=0
   NAS-Port-Type=Sync
   Acct-Status-Type=Stop
   Acct-Delay-Time=0
   Acct-Session-Id="262862705"
   Acct-Authentic=Local
   Acct-Session-Time=29
   Acct-Input-Octets=103
   Acct-Output-Octets=20
   Acct-Input-Packets=0
   Acct-Output-Packets=0
   Ascend-Disconnect-Cause=1
   Ascend-Connect-Progress=50
   Ascend-Xmit-Rate=0
   Ascend-Data-Rate=0
   Ascend-PreSession-Time=14
   Ascend-Pre-Input-Octets=0
   Ascend-Pre-Output-Octets=0
   Ascend-Pre-Input-Packets=0
   Ascend-Pre-Output-Packets=0
   Ascend-Modem-PortNo=1
   Ascend-Modem-SlotNo=8
   Calling-Station-Id="8005"
```

A Stop record sent by proxy

Following is an example of a shelf controller accounting proxy for an HDLC call:

```
Wed Nov 5 14:50:21 1999
    User-Name="joel-mhp"
    NAS-IP-Address=200.65.212.199
    NAS-Port=2272
    NAS-Port-Type=Sync
    Acct-Status-Type=Stop
    Acct-Delay-Time=0
    Acct-Session-Id="246212864"
    Acct-Authentic=RADIUS
    Acct-Session-Time=4
    Acct-Input-Octets=0
    Acct-Output-Octets=0
    Acct-Input-Packets=0
    Acct-Output-Packets=0
    Ascend-Disconnect-Cause=210
    Ascend-Connect-Progress=67
    Ascend-Data-Rate=0
    Ascend-PreSession-Time=0
    Ascend-Pre-Input-Octets=174
    Ascend-Pre-Output-Octets=204
    Ascend-Pre-Input-Packets=7 /
    Ascend-Pre-Output-Packets=8
    Framed-Protocol=PPP
    Framed-IP-Address=200.168.6.66
```

Reference to RADIUS Attributes

4

RADIUS attribute descriptions listed alphabetically 4-1

Free-RADIUS attributes and their RFC equivalents 4-170

Unused attributes 4-171

Outdated attributes 4-172

RADIUS attribute descriptions listed alphabetically

Each entry in this section provides information in the following format:

Attribute Name

Description: The Description text explains the attribute.

Usage: The Usage text explains the values you can specify for the attribute.

Example: The Example text presents an example of how to use the attribute.

Dependencies: The Dependencies text tells you what other information you need in order to specify the proper value for the attribute.

See Also: The See Also text points you to related information.

Note: All RADIUS attributes and settings are case sensitive. The name of a TAOS unit cannot contain embedded spaces.

Acct-Authentic (45)

Description: Indicates the method the TAOS unit used to authenticate a call, or reports that the TAOS unit accepted the call without authentication.

Usage: Acct-Authentic does not appear in a user profile. It can have one of the following values:

- None (0) indicates the TAOS unit accepted the call without authentication.
- RADIUS (1) indicates that RADIUS authenticated the incoming call. RADIUS is the default.

- Local (2) indicates that the TAOS unit authenticated the call by means of a local Connection profile, TACACS profile, or TACACS+ profile, or that the TAOS unit accepted the call without authentication.

Example: `Acct-Authentic=Local`

Dependencies: The TAOS unit sends Acct-Authentic in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of an authenticated session (Acct-Status-Type=Stop)

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Delay-Time (41)

Description: Indicates how many seconds the TAOS unit has been trying to send the Accounting packet.

Usage: Acct-Delay-Time does not appear in a user profile. Its default value is 0 (zero).

Example: `Acct-Delay-Time=18`

Dependencies: The TAOS unit sends Acct-Delay-Time in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session (when Acct-Status-Type=Stop)
- When a session has failed authentication (when Acct-Status-Type=Stop)

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Input-Octets (42)

Description: Indicates how many octets the TAOS unit received during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Acct-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Example: `Acct-Input-Octets=2421`

Dependencies: The TAOS unit sends Acct-Input-Octets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session has been authenticated.
- The connection was asynchronous.

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Input-Packets (47)

Description: Indicates how many packets the TAOS unit received during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Acct-Input-Packets does not appear in a user profile. Its default value is 0 (zero).

Example: `Acct-Input-Packets=79`

Dependencies: The TAOS unit sends Acct-Input-Packets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session has been authenticated.
- A framed protocol is in use.

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Link-Count (51)

Description: Indicates the number of channels that have ever been in the Multilink bundle, even if those channels are spread across multiple machines in a stacked environment.

Usage: Acct-Link-Count does not appear in a user profile and has no default value.

Example: `Acct-Link-Count=5`

Dependencies: The TAOS unit sends Acct-Link-Count in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Multi-Session-Id (50)

Description: Specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call.

Usage: Acct-Multi-Session-Id is a string value. It does not appear in a user profile and has no default value.

Example: `Acct-Multi-Session-Id=1234`

Dependencies: The TAOS unit sends Acct-Multi-Session-ID in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Output-Octets (43)

Description: Indicates how many octets the TAOS unit has sent during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Acct-Output-Octets does not appear in a user profile. Its default value is 0 (zero).

Example: `Acct-Output-Octets=1517`

Dependencies: The TAOS unit sends Acct-Output-Octets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session has been authenticated.
- The connection was asynchronous.

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Output-Packets (48)

Description: Indicates how many packets the TAOS unit has sent during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Acct-Output-Packets does not appear in a user profile. Its default value is 0 (zero).

Example: `Acct-Output-Packets=47`

Dependencies: The TAOS unit sends Acct-Output-Packets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session is authenticated.
- A framed protocol is in use.

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Session-Id (44)

Description: Identifies the routing or terminal-server session reported in the Accounting-Request packet. RADIUS correlates the Accounting Start packet and Accounting Stop packet by means of Acct-Session-Id.

Usage: Acct-Session-Id does not appear in a user profile. Its value is a random number with a range from 1 to 2,137,383,647. For every session, RADIUS generates a unique session ID.

Example: `Acct-Session-Id="1234567"`

Dependencies: The TAOS unit sends Acct-Session-Id in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session (when Acct-Status-Type=Stop)
- When a session has failed authentication (when Acct-Status-Type=Stop)

In addition, consider the following:

- When an SNMP accounting session and a RADIUS accounting session have the same ID, they are identical. However, SNMP records all calls, while RADIUS records only those calls that result in a successful login or authentication.
- At the TAOS configuration interface, you can specify whether the numeric base of the Acct-Session-Id attribute is 10 or 16.

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Session-Time (46)

Description: Indicates how many seconds the session has been logged in. For an outgoing IP-Fax call, the time period begins when the modem is reserved and ends when the call is terminated.

Usage: Acct-Session-Time does not appear in a user profile. Its default value is 0 (zero).

Example: `Acct-Session-Time=128`

Dependencies: The TAOS unit sends Acct-Session-Time in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when the session has been authenticated.

See Also: "Acct-Status-Type (40)" on page 4-5.

Acct-Status-Type (40)

Description: Indicates the type of accounting packet that the TAOS unit sends to the RADIUS server in an Accounting-Request packet.

Usage: Acct-Status-Type does not appear in a user profile. It can have one of the following values:

- Start (1) indicates a Start packet sent at the beginning of a session.
- Stop (2) indicates a Stop packet sent at the end of a session or when a session fails authentication.
- Checkpoint (3) indicates a Checkpoint packet.
- Accounting-On (7) specifies that accounting has been enabled.
- Accounting-Off (8) specifies that accounting has been disabled.

Example: `Acct-Status-Type=Stop`

See Also: "Acct-Session-Id (44)" on page 4-4.

Ascend-Add-Seconds (240)

Description: Specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Ascend-Target-Util attribute before the TAOS unit begins adding bandwidth to a session. The TAOS unit determines the ALU for a session by applying the algorithm specified by the Ascend-History-Weigh-Type attribute.

When utilization exceeds the threshold for a period greater than the value of the Ascend-Add-Seconds attribute, the TAOS unit attempts to add the number of channels specified by the Ascend-Inc-Channel-Count attribute. Using the Ascend-Add-Seconds attribute prevents the system from continually adding bandwidth and can slow down the process of allocating bandwidth.

Usage: Specify an integer from 1 to 300. The default value is 5.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation™ (DBA), including Ascend-Add-Seconds:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- Additional channels must be available, and the number of channels the TAOS unit adds cannot exceed the number specified by the Ascend-Maximum-Channels attribute.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value. If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

See Also: "Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Appletalk-Peer-Mode (117)

Description: Specifies whether the connection is for a single dial-in station or for a router.

Usage: Specify one of the following values:

- Appletalk-Peer-Router (0) specifies that the caller is an AppleTalk router.

- Appletalk-Peer-Dialin (1) specifies that the caller is a dial-in AppleTalk client.

Example: The following example shows a RADIUS user profile for a routed connection:

```
unit50  User-Password="mypw"
        Service-Type=Framed-User,
        Framed-Protocol=PPP,
        Ascend-Appletalk-Peer-Mode=Appletalk-Peer-Router,
        Ascend-Route-Appletalk=Route-Appletalk-Yes
```

The following is an example of a RADIUS user profile for a dial-in connection:

```
mac1    User-Password="mac1"
        Service-Type=Framed-User,
        Framed-Protocol=PPP,
        Ascend-Appletalk-Peer-Mode=Appletalk-Peer-Dialin,
        Ascend-Route-Appletalk=Route-Appletalk-Yes
```

Dependencies: Ascend-Route-Appletalk must be set to Route-Appletalk-Yes.

See Also: "Ascend-Appletalk-Route (116)" on page 4-7.

Ascend-Appletalk-Route (116)

Description: Defines a static AppleTalk route in a RADIUS pseudo-user profile.

Usage: Create a pseudo-user profile with the first line in the following format:

`appleroute-`*`num`* `User-Password="ascend", Service-Type=Outbound-User`

where *num* is a number in a series starting at 1. Then, enter one or more static AppleTalk route specifications in the following format:

`Ascend-Appletalk-Route="`*`net_start net_end zone_name profile_name`*`"`

Table 4-1 describes each argument.

Table 4-1. Ascend-Appletalk-Route arguments

Argument	Specifies
net_start	The lower limit of the network range for this network. A network range is a range of network numbers set into the port descriptor of the router port and then transmitted through RTMP to the other nodes of the network. Each of the numbers within a network range can represent up to 253 devices. The default is null.
net_end	The upper limit of the network range for this network. This range defines the networks available for packets routed by means of the static route. Specify a number between 1 and 65199. If there are other AppleTalk routers on the network, you must configure the network ranges to be identical to the ranges specified on the other routers.

Table 4-1. Ascend-Appletalk-Route arguments (continued)

Argument	Specifies
zone_name	The name of the AppleTalk zone associated with this network. A zone is a multicast address containing a subset of the AppleTalk nodes on an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand. In the Ascend AppleTalk router, zone names are case insensitive. However, because some routers regard zone names as case sensitive, the spelling of zone names should be consistent when you configure multiple connections or routers. You can use up to 33 alphanumeric characters. The default is null.
profile_name	The outgoing RADIUS user profile that the route uses. The default is null.

Each static route must appear in a pseudo-user profile. User profile entries for Appletalk static routes are identified by the special name `appleroute-#` and have the following format:

```
appleroute-# User-Password="ascend" Service-Type=Outbound-User
   Address 1
   Address 2
   ...
   Address n
```

`Address` *n* is the actual route associated with this entry.

Example: Following is an example of a static route with its associated user profile:

```
appleroute-1  User-Password="ascend" Service-Type=Outbound-User
Ascend-Appletalk-Route="20 25 testzone1 unit50"

unit50  User-Password="ascend" Service-Type=Framed-User,
        Framed-Protocol=MPP,
        Ascend-Appletalk-Peer-Mode=Appletalk-Peer-Router,
        Ascend-Route-Appletalk=Route-Appletalk-Yes,
        Ascend-Dialout-Allowed=Dialout-Allowed,
        Ascend-Dial-Number="83272",
        Ascend-Send-Auth=Send-Auth-PAP,
        Ascend-Send-Passwd="TAOS"
```

Dependencies: Ascend-Route-Appletalk must be set to Route-Appletalk-Yes.

See Also: "Ascend-Appletalk-Peer-Mode (117)" on page 4-6.

Ascend-ARA-PW (181)

Description: Specifies the password of the incoming caller over an AppleTalk Remote Access (ARA) connection. The ARA software in the TAOS unit uses Data Encryption Standard (DES) to encrypt and decrypt the password.

Usage: Specify an alphanumeric text string containing up to 20 characters. The default value is null. The password you enter for this attribute must be identical to the password you enter in the first line of the user profile. The TAOS unit requires both entries.

Example: This example shows how to set up a TCP connection through ARA with a dynamic IP address assignment:

```
Emma User-Password="pwd"
     Framed-Protocol=ARA,
     Ascend-ARA-PW="pwd",
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Assign-IP-Pool=1
```

See Also: "User-Password (2)" on page 4-168.

Ascend-Assign-IP-Client (144)

Description: Specifies the IP address of a unit allowed to access the global address pools managed by RADIPAD.

Usage: Specify an IP address. You can specify multiple instances of the Ascend-Assign-IP-Client attribute.

Example: The following profile specifies two RADIPAD clients:

```
radipa-hosts User-Password="ascend", Service-Type=Outbound-User
   Ascend-Assign-IP-Server=10.31.4.34,
   Ascend-Assign-IP-Client=10.31.4.10,
   Ascend-Assign-IP-Client=10.31.4.11
```

See Also: "Ascend-Assign-IP-Global-Pool (146)" on page 4-9 and "Ascend-Assign-IP-Server (145)" on page 4-10.

Ascend-Assign-IP-Global-Pool (146)

Description: Specifies the global address pool from which RADIUS should assign each user an address.

A dynamic address comes from the pool of addresses you set up on the TAOS unit, the Ascend-IP-Pool-Definition attribute in a RADIUS profile, or both. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the TAOS configuration interface, but only if you designate the two pools by the same number.

Usage: Specify the name of the pseudo-user profile containing global IP pool definitions. The TAOS unit tries to allocate an address from the pools in order and chooses an address from the pool with the first available IP address.

Example: In the following user profile, the host requests an address from the global address pool configured in the pseudo-user profile called global-pool-Alameda:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
```

```
     Framed-Routing=None,
     Ascend-Assign-IP-Global-Pool="Global-Pool-Alameda"
```

Dependencies: Do not set the Framed-IP-Address attribute in the user profile. If you do, the TAOS unit requires the caller to use the static IP address the attribute specifies.

See Also: "Ascend-IP-Pool-Definition (217)" on page 4-93.

Ascend-Assign-IP-Pool (218)

Description: Specifies the address pool from which RADIUS assigns the user an IP address.

A dynamic address comes from the pool of addresses you set up on the TAOS unit, the Ascend-IP-Pool-Definition attribute in a RADIUS profile, or both. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the TAOS configuration interface, but only if you designate the two pools by the same number.

Usage: Specify an integer corresponding to an address pool. The default value is 0 (zero). If you accept the default, RADIUS chooses an address from any pool that has one available.

Example: In the following user profile, the host requests an address from pool #2:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Assign-IP-Pool=2
```

See Also: "Ascend-IP-Pool-Definition (217)" on page 4-93.

Ascend-Assign-IP-Server (145)

Description: Specifies the IP address of the host running `radipad`.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. Only one instance of the attribute can appear in the profile. The default value is a placeholder only. You must specify a valid IP address for `radipad` to work.

Example: The following profile specifies a RADIPAD server at IP address 10.31.4.34:

```
radipa-hosts User-Password="ascend", Service-Type=Outbound-User
   Ascend-Assign-IP-Server=10.31.4.34,
   Ascend-Assign-IP-Client=10.31.4.10,
   Ascend-Assign-IP-Client=10.31.4.11
```

See Also: "Ascend-Assign-IP-Global-Pool (146)" on page 4-9 and "Ascend-Assign-IP-Client (144)" on page 4-9.

Ascend-ATM-Connect-Group (63)

Description: Specifies the nailed group for the second leg of an Asynchronous Transfer Mode (ATM) circuit.

Usage: Specify an integer.

Example: The following profile specifies nailed group 200 for the second leg of an ATM circuit:

```
permconn-TAOS100-2 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-CIR,
        User-Name="Test103",
        Ascend-ATM-Group=225,
        Ascend-Route-IP=Route-IP-No,
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=33,
        Ascend-ATM-Connect-Vpi=10,
        Ascend-ATM-Connect-Vci=200,
        Ascend-ATM-Connect-Group=200,
        Ascend-QOS-Upstream="qos1",
        Ascend-QOS-Downstream="qos2"
```

See Also: "Ascend-ATM-Group (64)" on page 4-14.

Ascend-ATM-Connect-Vci (62)

Description: Specifies the Virtual Channel Identifier (VCI) for the second leg of an Asynchronous Transfer Mode (ATM) circuit.

Usage: Specify a value from 32 to 1023. The default is 32. The maximum setting is determined by TAOS hardware capabilities.

Example: The following profile specifies VCI 200 for the second leg of an ATM circuit:

```
permconn-TAOS100-2 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-CIR,
        User-Name="Test103",
        Ascend-ATM-Group=225,
        Ascend-Route-IP=Route-IP-No,
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=33,
        Ascend-ATM-Connect-Vpi=10,
        Ascend-ATM-Connect-Vci=200,
        Ascend-ATM-Connect-Group=200,
        Ascend-QOS-Upstream="qos1",
        Ascend-QOS-Downstream="qos2"
```

See Also: "Ascend-ATM-Vci (95)" on page 4-15.

Ascend-ATM-Connect-Vpi (61)

Description: Specifies the Virtual Path Identifier (VPI) for the second leg of an Asynchronous Transfer Mode (ATM) circuit.

Usage: Specify a value from 0 to 15. The default is 0 (zero).

Example: The following profile specifies VPI 10 for the second leg of an ATM circuit:

```
permconn-TAOS100-2 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-CIR,
        User-Name="Test103",
        Ascend-ATM-Group=225,
        Ascend-Route-IP=Route-IP-No,
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=33,
        Ascend-ATM-Connect-Vpi=10,
        Ascend-ATM-Connect-Vci=200,
        Ascend-ATM-Connect-Group=200,
        Ascend-QOS-Upstream="qos1",
        Ascend-QOS-Downstream="qos2"
```

See Also: "Ascend-ATM-Vpi (94)" on page 4-15.

Ascend-ATM-Direct (76)

Description: Specifies whether ATM-Direct is enabled.

Usage: Specify one of the following settings:

- ATM-Direct-Yes (1) specifies that ATM-Direct is enabled.
- ATM-Direct-No (0) specifies that ATM-Direct is disabled.

Example: The following profiles configure ATM-Direct for incoming calls:

```
caller-1 User-Password="caller1*3", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.5.6.7,
    Framed-IP-Netmask=255.255.255.255
    Ascend-ATM-Direct=ATM-Direct-Yes,
    Ascend-ATM-Direct-Profile="atm-switch-1"

caller-2 User-Password="caller2!!8", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.7.8.9,
    Framed-IP-Netmask=255.255.255.255
    Ascend-ATM-Direct=ATM-Direct-Yes,
    Ascend-ATM-Direct-Profile="atm-switch-1"
```

See Also: "Ascend-ATM-Direct-Profile (77)" on page 4-12.

Ascend-ATM-Direct-Profile (77)

Description: Specifies the host name of the ATM interface to which data will be switched.

Usage: Specify a text string.

Example: In the following profiles, the name of the profile for the connection to the ATM switch is `atm-switch-1`:

```
caller-1 User-Password="caller1*3", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.5.6.7,
```

```
    Framed-IP-Netmask=255.255.255.255
    Ascend-ATM-Direct=ATM-Direct-Yes,
    Ascend-ATM-Direct-Profile="atm-switch-1"
caller-2 User-Password="caller2!!8", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.7.8.9,
    Framed-IP-Netmask=255.255.255.255
    Ascend-ATM-Direct=ATM-Direct-Yes,
    Ascend-ATM-Direct-Profile="atm-switch-1"
```

Dependencies: If Ascend-ATM-Direct is set to ATM-Direct-Yes, you must specify a value for Ascend-ATM-Direct-Profile.

See Also: "Ascend-ATM-Direct (76)" on page 4-12.

Ascend-ATM-Fault-Management (14)

Description: Specifies the type of fault management associated with an Asynchronous Transfer Mode (ATM) Virtual Circuit (VC).

Usage: Specify one of the following values:

- VC-No-Loopback (0) specifies that no fault management takes place.
- VC-Segment-Loopback (1) specifies that the unit monitors the VC by sending F5-segment loopback cells once every five seconds.
- VC-End-To-End-Loopback (2) specifies that the unit monitors the VC by sending F5 end-to-end loopback cells once every five seconds.

Example: The following profile specifies end-to-end loopback:

```
permconn-yossi-1 User-Password="ascend", Service-Type=Outbound-User
   Framed-Protocol=ATM-FR-CIR,
   Framed-IP-Address=222.222.222.1,
   Framed-IP-Netmask=255.255.255.0,
   Ascend-FR-Profile-Name="atm-30-sw",
   Ascend-Metric=2,
   Framed-Routing=None,
   Ascend-Group="70",
   Acct-Authentic=None,
   Ascend-Send-Auth=Send-Auth-None,
   Ascend-Call-Type=Nailed,
   Ascend-FT1-Caller=FT1-Yes,
   Ascend-Route-IP=Route-IP-No,
   Ascend-ATM-Vpi=1,
   Ascend-ATM-Vci=43,
   Ascend-ATM-Fault-Management=VC-End-To-End-Loopback,
   Ascend-ATM-Loopback-Cell-Loss=5,
   Ascend-FR-Circuit-Name="adsl-atm",
   Ascend-Data-Svc=Nailed-64K
```

See Also: "Ascend-ATM-Loopback-Cell-Loss (15)" on page 4-14.

Ascend-ATM-Group (64)

Description: Specifies the nailed group for the first leg of an Asynchronous Transfer Mode (ATM) circuit.

Usage: Specify an integer.

Example: The following profile specifies nailed group 5 for the first leg of an ATM circuit:

```
permconn-TAOS100-2 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-CIR,
        User-Name="Test103",
        Ascend-ATM-Group=225,
        Ascend-Route-IP=Route-IP-No,
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=33,
        Ascend-ATM-Group=5,
        Ascend-ATM-Connect-Vpi=10,
        Ascend-ATM-Connect-Vci=200,
        Ascend-ATM-Connect-Group=200,
        Ascend-QOS-Upstream="qos1",
        Ascend-QOS-Downstream="qos2"
```

See Also: "Ascend-ATM-Connect-Group (63)" on page 4-10,
"Ascend-ATM-Connect-Vci (62)" on page 4-11,
"Ascend-ATM-Connect-Vpi (61)" on page 4-11,
"Ascend-ATM-Fault-Management (14)" on page 4-13, and
"Ascend-ATM-Loopback-Cell-Loss (15)" on page 4-14.

Ascend-ATM-Loopback-Cell-Loss (15)

Description: Specifies the number of consecutive loopback cell that can be lost before the unit clears the Virtual Circuit (VC).

Usage: Specify an integer.

Example: The following profile specifies that the unit clears the VC after five consecutive cells have been lost:

```
permconn-yossi-1 User-Password="ascend", Service-Type=Outbound-User
   Framed-Protocol=ATM-FR-CIR,
   Framed-IP-Address=222.222.222.1,
   Framed-IP-Netmask=255.255.255.0,
   Ascend-FR-Profile-Name="atm-30-sw",
   Ascend-Metric=2,
   Framed-Routing=None,
   Ascend-Group="70",
   Acct-Authentic=None,
   Ascend-Send-Auth=Send-Auth-None,
   Ascend-Call-Type=Nailed,
   Ascend-FT1-Caller=FT1-Yes,
   Ascend-Route-IP=Route-IP-No,
   Ascend-ATM-Vpi=1,
   Ascend-ATM-Vci=43,
```

```
   Ascend-ATM-Fault-Management=VC-End-To-End-Loopback,
   Ascend-ATM-Loopback-Cell-Loss=5,
   Ascend-FR-Circuit-Name="adsl-atm",
   Ascend-Data-Svc=Nailed-64K
```

See Also: "Ascend-ATM-Fault-Management (14)" on page 4-13.

Ascend-ATM-Vci (95)

Description: Specifies the Virtual Channel Identifier (VCI) for the first leg of an Asynchronous Transfer Mode (ATM) connection.

Usage: Specify a value from 32 to 1023. The default is 32. The maximum setting is determined by TAOS hardware capabilities.

Example: The following profile specifies VCI 43 for the first leg of an ATM circuit:

```
permconn-yossi-1 User-Password="ascend", Service-Type=Outbound-User
   Framed-Protocol=ATM-FR-CIR,
   Framed-IP-Address=222.222.222.1,
   Framed-IP-Netmask=255.255.255.0,
   Ascend-FR-Profile-Name="atm-30-sw",
   Ascend-Metric=2,
   Framed-Routing=None,
   Ascend-Group="70",
   Acct-Authentic=None,
   Ascend-Send-Auth=Send-Auth-None,
   Ascend-Call-Type=Nailed,
   Ascend-FT1-Caller=FT1-Yes,
   Ascend-Route-IP=Route-IP-No,
   Ascend-ATM-Vpi=1,
   Ascend-ATM-Vci=43,
   Ascend-FR-Circuit-Name="adsl-atm",
   Ascend-Data-Svc=Nailed-64K
```

See Also: "Ascend-ATM-Vpi (94)" on page 4-15 and "Framed-Protocol (7)" on page 4-149.

Ascend-ATM-Vpi (94)

Description: Specifies the Virtual Path Identifier (VPI) for the first leg of an Asynchronous Transfer Mode (ATM) connection.

Usage: Specify a value from 0 to 15. The default is 0 (zero).

Example: The following profile specifies VPI 1 for the first leg of an ATM circuit:

```
permconn-yossi-2 User-Password="ascend", Service-Type=Outbound-User
   Framed-Protocol=ATM-1483,
   Framed-IP-Address=222.222.222.1,
   Framed-IP-Netmask=255.255.255.0,
   Ascend-FR-Profile-Name="atm-30",
   Ascend-Metric=2,
   Framed-Routing=None,
   Ascend-Group="70",
```

```
Acct-Authentic=None,
Ascend-Send-Auth=Send-Auth-None,
Ascend-Call-Type=Nailed,
Ascend-FT1-Caller=FT1-Yes,
Ascend-Route-IP=Route-IP-Yes,
Ascend-ATM-Vpi=1,
Ascend-ATM-Vci=42,
Ascend-Data-Svc=Nailed-64K
```

See Also: "Ascend-ATM-Vci (95)" on page 4-15 and "Framed-Protocol (7)" on page 4-149.

Ascend-Authen-Alias (203)

Description: Sets the TAOS unit's login name during PPP authentication. When the TAOS unit places an outgoing call, it identifies itself by a login name and password. The login name is either its system name or the value you specify for the Ascend-Authen-Alias attribute.

Usage: Specify a text string of up to 16 characters, with no spaces.

Example: The following example shows how to use the Ascend-Authen-Alias attribute in an outgoing profile:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
      User-Name="Homer",
      Ascend-Authen-Alias="myunitcallingU",
      Ascend-Send-Auth=Send-Auth-PAP,
      Ascend-Send-Secret="passwrd1",
      Ascend-Dial-Number="31",
      Framed-Protocol=PPP,
      Framed-IP-Address=10.0.100.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Metric=2,
      Framed-Routing=None,
      Framed-Route="10.5.0.0/24 10.0.100.1 1"
```

Ascend-Auth-Type (81)

Description: Specifies the type of PPP authentication the connection uses during tier-1 Calling-Line ID (CLID) or Dialed Number Information Service (DNIS) authentication.

Usage: Specify one of the following settings:

- Auth-None (0) specifies that no tier-2 name and password authentication is required. Specifying this value has the same effect as setting Ascend-Require-Auth to Not-Require-Auth.
- Auth-Default (1) specifies that the connection uses the Receive-Auth-Mode setting.
- Auth-Any (2) specifies that the connection must use PAP, CHAP or MS-CHAP.
- Auth-PAP (3) specifies that the connection must use PAP. The remote end sends its password in the clear. The password is not encrypted.
- Auth-CHAP (4) specifies that the connection must use CHAP. The remote end does not send its password in the clear. An MD5 digest calculated from the password and a random challenge are sent instead.

- Auth-MS-CHAP (5) specifies that connection must use MS-CHAP.

Example: In the following pseudo-user profile, bidirectional CHAP authentication is required:

```
111886067 User-Password="Ascend-CLID"
    Service-Type=Framed-User
    Ascend-Require-Auth=Require-Auth
    Ascend-Auth-Type=Auth-CHAP
    Ascend-Send-Auth=Send-Auth-CHAP
    Ascend-Bi-Directional-Auth=Bi-Directional-Auth-Required
```

See Also: "Ascend-Require-Auth (201)" on page 4-125 and "Ascend-Send-Auth (231)" on page 4-130.

Ascend-Backup (176)

Description: Specifies the name of a backup profile for a nailed-up link.

Usage: Specify the name of the profile that you want to act as the backup. The backup connection can be switched or nailed up. The default value is null.

Example: In the following pseudo-user profile, the backup profile is called `Backup1`:

```
permconn-SanFran-1 User-Password="ascend", Service-Type=Outbound-User
       User-Name="LA",
       Framed-Protocol=PPP,
       Framed-IP-Address=50.1.1.2,
       Framed-IP-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Call-Type=Nailed,
       Ascend-Group="1",
       Ascend-FT1-Caller=FT1-Yes,
       Ascend-Backup="Backup1"
```

Dependencies: Consider the following:

- The Ascend-Backup attribute applies to nailed-up connections only (Ascend-Call-Type=Nailed or Nailed/Mpp).
- Do not create nested backup connections.
- When you use the backup connection, the TAOS unit does not move routes to the backup profile. Therefore, the IP routes that appear in the terminal-server display might be incorrect, although statistical counts reflect the change.
- Do not use the Ascend-Backup attribute to provide alternative lines for getting to a single destination.
- The profile for a backup interface does not inherit features, such as filters or firewalls, from the profile for the primary nailed-up connection.

Ascend-BACP-Enable (133)

Description: Specifies whether Bandwidth Allocation Control Protocol (BACP) is enabled for the link. BACP provides Dynamic Bandwidth Allocation (DBA) for MP-encapsulated digital or analog links. Described in RFC 2125, BACP is the Internet standard protocol equivalent to the MP+ bandwidth allocation protocol. BACP functions similarly to MP+, and BACP connections use the same attributes as MP+ links.

Usage: Specify one of the following settings:

- BACP-No (0) disables BACP for the link. BACP-No is the default.
- BACP-Yes (1) enables BACP for the link.

Example: The following user profile specifies that BACP is enabled for the link:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Ascend-BACP-Enable=BACP-Yes,
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: For DBA to work on an MP connection, both sides of the connection must support BACP.

See Also: "Framed-Protocol (7)" on page 4-149.

Ascend-Base-Channel-Count (172)

Description: Specifies the initial number of channels the TAOS unit sets up when originating calls for a PPP, MP, or MP+ link.

Usage: The maximum number of channels you can specify depends upon the nature of the link:

- For a PPP link, the maximum number of channels is always 1.
- For an MP+ or MP link, you can specify any value up to the number of channels available, but the device at the remote end of the link must also support MP+ or MP.

The default value is 1.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Base-Channel-Count:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
```

```
Framed-IP-Address=200.0.5.1,
Framed-IP-Netmask=255.255.255.0,
Ascend-Target-Util=80,
Ascend-History-Weigh-Type=History-Constant,
Ascend-Seconds-Of-History=90,
Ascend-Base-Channel-Count=2,
Ascend-Add-Seconds=30,
Ascend-Remove-Seconds=30,
Ascend-Minimum-Channels=2,
Ascend-Maximum-Channels=10,
Ascend-Inc-Channel-Count=2,
Ascend-Dec-Channel-Count=2,
Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: The Ascend-Base-Channel-Count attribute does not apply when all channels of the link are nailed up (Ascend-Call-Type=Nailed).

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Bi-Directional-Auth (46)

Description: Specifies whether CHAP authentication must be bidirectional.

Usage: Ascend-Bi-Directional-Auth appears in an Access-Accept packet. Specify one of the following values:

- Bi-Directional-Auth-None (0) specifies that authentication is unidirectional. The called device identifies the calling one. The TAOS unit prevents the authentication in which the calling party identifies the called party.
- Bi-Directional-Auth-Allowed (1) specifies that authentication can be bidirectional.

  When the TAOS unit is the called device, the TAOS unit identifies the calling device. The system also allows the calling device to authenticate the TAOS unit, but this authentication is not mandatory. Therefore, if the calling device does not authenticate the TAOS unit, the TAOS unit can still accept the call.

  When the TAOS unit is the calling device, the TAOS unit answers the authentication initiated by the called device. The TAOS unit tries to negotiate authentication in the opposite direction as well, but if the called device refuses this second authentication option, the call is still established.
- Bi-Directional-Auth-Required (2) specifies that authentication must be bidirectional. The TAOS unit requires that both the calling and called devices authenticate each other. If authentication is not performed in both directions, the TAOS unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).

Example: In the following profile, bidirectional authentication is required:

```
111886067 User-Password="Ascend-CLID", Service-Type=Framed-User
          Ascend-Require-Auth=Require-Auth,
          Ascend-Auth-Type=Auth-CHAP,
          Ascend-Send-Auth=Send-Auth-CHAP,
          Ascend-Bi-Directional-Auth=Bi-Directional-Auth-Required
```

Dependencies: Bidirectional authentication is applicable only if the authentication mode is CHAP, MS-CHAP, or CACHE-TOKEN. If you specify Bi-Directional-Auth-Allowed or Bi-Directional-Auth-Required, and the second authentication is attempted, it must be successful. Otherwise, the TAOS unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).

See Also: "Ascend-Recv-Name (45)" on page 4-122.

Ascend-Billing-Number (249)

Description: Specifies a billing number for charges incurred on the line. If you do not enter a billing number, the telephone company assigns charges to the telephone number associated with the line. Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own Ascend-Billing-Number, your carrier can separate and tally each department's usage.

Usage: Specify a telephone number of up to ten characters, limited to the following:

```
1234567890()[]!z-*# |
```

Example: In the following pseudo-user profile, the billing number is 555-5555:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
     User-Name="Homer",
     Ascend-Dial-Number=555-3131,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.0.100.1,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Billing-Number=555-5555
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

Dependencies: The TAOS unit uses the Ascend-Billing-Number attribute differently for different types of lines:

- For a T1 line, the TAOS unit appends the value specified in the Ascend-Billing-Number attribute to the end of each phone number it dials for the call.
- Ascend-Billing-Number for outgoing calls applies only to installations in Australia.
- For a T1 PRI line, the TAOS unit uses the value of Ascend-Billing-Number rather than the phone number to identify itself to the answering party. In this situation, the Calling-Line ID (CLID) that the answering side receives is not the true phone number of the caller. This situation presents a security breach if you use CLID-Auth-Mode.

If you specify a value for the Ascend-Billing-Number attribute, there is no guarantee that the phone company will send it to the answering device.

See Also: "Calling-Station-Id (31)" on page 4-145.

Ascend-BIR-Bridge-Group (72)

Description: Specifies a bridge group for a Bridged IP Routing (BIR) connection.

Usage: Specify an integer from 1 to 2000.

Example: The following profile specifies bridge group 10 for a BIR connection over a Frame Relay link:

```
permconn-Jim-2 User-Password="ascend"
         Service-Type=Outbound-User,
         Framed-Protocol=FR,
         User-Name="cpe2-radius",
         Ascend-Route-IP=Route-IP-No,
         Framed-Routing=None,
         Ascend-Call-Type=Nailed,
         Ascend-Bridge=Bridge-Yes,
         Ascend-BIR-Bridge-Group=10,
         Ascend-FR-Profile-Name="frm2-rad"
```

See Also: "Ascend-BIR-Enable (70)" on page 4-21
and "Ascend-BIR-Proxy (71)" on page 4-22.

Ascend-BIR-Enable (70)

Description: Enables or disables Bridged IP Routing (BIR).

Usage: Specify one of the following values:

- BIR-Enable-No (0) disables BIR.
- BIR-Enable-Yes (1) enables BIR.

Example: The following profile enables BIR over a Frame Relay link:

```
permconn-Gabi-1 User-Password="ascend"
         Service-Type=Outbound-User,
         Framed-Protocol=FR,
         User-Name="cpe1-radius",
         Framed-Routing=None,
         Framed-IP-Address=10.10.10.2,
         Framed-IP-Netmask=255.255.255.255,
         Ascend-Call-Type=Nailed,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-PPP-Address=10.10.10.1,
         Ascend-IF-Netmask=255.255.255.0,
         Ascend-BIR-Enable=BIR-Enable-Yes,
         Ascend-BIR-Proxy=BIR-Proxy-Yes,
         Ascend-FR-Profile-Name="frm1-rad"
```

See Also: "Ascend-BIR-Bridge-Group (72)" on page 4-21 and
"Ascend-BIR-Proxy (71)" on page 4-22.

Ascend-BIR-Proxy (71)

Description: Specifies whether proxy ARP is enabled for the Bridged IP Routing (BIR) connection.

Usage: Specify one of the following values:

- BIR-Proxy-No (0) disables proxy ARP for the BIR connection.
- BIR-Proxy-Yes (1) enables proxy ARP for the BIR connection.

Example: The following profile enables proxy ARP for a BIR connection over Frame Relay:

```
permconn-Gabi-1 User-Password="ascend"
         Service-Type=Outbound-User,
         Framed-Protocol=FR,
         User-Name="cpe1-radius",
         Framed-Routing=None,
         Framed-IP-Address=10.10.10.2,
         Framed-IP-Netmask=255.255.255.255,
         Ascend-Call-Type=Nailed,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-PPP-Address=10.10.10.1,
         Ascend-IF-Netmask=255.255.255.0,
         Ascend-BIR-Enable=BIR-Enable-Yes,
         Ascend-BIR-Proxy=BIR-Proxy-Yes,
         Ascend-FR-Profile-Name="frm1-rad"
```

See Also: "Ascend-BIR-Bridge-Group (72)" on page 4-21 and
"Ascend-BIR-Enable (70)" on page 4-21.

Ascend-Bridge (230)

Description: Enables or disables protocol-independent bridging for the user profile.

Usage: Specify one of the following values:

- Bridge-No (0) disables bridging for the link. Bridge-No is the default.
- Bridge-Yes (1) enables bridging for the link.

Example: The following user profile specifies an IPX bridging link:

```
TAOS1 User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Client,
     Ascend-Netware-timeout=30
```

See Also: "Ascend-Bridge-Address (168)" on page 4-23.

Ascend-Bridge-Address (168)

Description: Specifies the IP address and associated MAC address of a remote device to which the TAOS unit can form a bridging connection.

Usage: The Ascend-Bridge-Address attribute has the following format:

```
Ascend-Bridge-Address="MAC_address profile_name IP_address"
```

Table 4-2 describes the Ascend-Bridge-Address arguments.

Table 4-2. Ascend-Bridge-Address arguments

Argument	Specifies
MAC_address	MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, `:y` is the same as `:0y`. The default value is 000000000000.
profile_name	Name of the dialout profile the TAOS unit uses to bring up the connection. You can specify a local profile or a RADIUS user profile. The TAOS unit looks for a local profile first.
IP_address	IP address in dotted decimal notation. The default value is 0.0.0.0.

When your TAOS unit receives an ARP request for one of the IP addresses you specify, the unit replies with the corresponding MAC address and uses the specified profile to bring up a connection to that address. Because the TAOS unit replies to these ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

Example: Following is a pseudo-user profile containing two bridging table entries:

```
Bridge-Ascend-1 User-Password="Ascend", Service-Type=
Outbound-User
       Ascend-Bridge-Address="2:2:3:10:11:12 Prof1 1.2.3.4 1",
       Ascend-Bridge-Address="2:2:3:13:14:15 Prof2 5.6.7.8 2"
```

Dependencies: Each bridge entry must appear in a pseudo-user profile. You create a pseudo-user profile to store information that the TAOS unit can query—in this case, in order to store bridging information. For a unit-specific bridge entry, specify the first line of a pseudo-user profile in this format:

```
Bridge-unit_name-num User-Password="Ascend", Service-Type=
Outbound-User
```

The *unit_name* argument is the system name of the TAOS unit. The *num* argument is a number in a sequential series, starting at 1.

In each pseudo-user profile, you specify one or more Ascend-Bridge-Address attributes. Whenever you power on or reset the TAOS unit, RADIUS adds bridging entries to the bridge table in the following way:

1. RADIUS looks for profiles having the format `Bridge-`*`unit_name-num`*, where *`unit_name`* is the system name and *`num`* is a number in a sequential series, starting with 1.
2. RADIUS loads the data to create the bridging tables.

See Also: "Ascend-Bridge (230)" on page 4-22.

Ascend-Bridge-Non-PPPoE (75)

Description: Specifies whether packets having Ethernet types other than PPP over Ethernet (PPPoE) should be bridged on the connection.

Usage: Specify one of the following settings:

- Bridge-Non-PPPoE-No (0) specifies that non-PPPoE packets are not bridged.
- Bridge-Non-PPPoE-Yes (1) specifies that non-PPPoE packets are bridged.

Example: The following profile specifies that the unit does not bridge non-PPPoE Ethernet packets over the ATM connection:

```
permconn-Yossi-1 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-1483,
        User-Name="b-rad-pppoe",
        Framed-Routing=None,
        Acct-Authentic=None,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-Group="2",
        Ascend-Call-Type=Nailed,
        Ascend-Route-IP=Route-IP-No,
        Ascend-Bridge=Bridge-Yes,
        Ascend-ATM-Vpi=15,
        Ascend-ATM-Vci=35,
        Ascend-Data-Svc=Nailed-64K,
        Ascend-PPPoE-Enable=PPPoE-Yes,
        Ascend-Bridge-Non-PPPoE=Bridge-Non-PPPoE-No
```

See Also: "Ascend-PPPoE-Enable (74)" on page 4-113.

Ascend-Cache-Refresh (56)

Description: Specifies whether the cache timer is reset each time a new session that refers to a pseudo-user profile becomes active.

Usage: Specify one of the following values:

- Refresh-No (0) specifies that the cache timer is not reset.
- Refresh-Yes (1) specifies that the cache timer is reset.

Example: The following specifies that references to a cached filter profile reset its cache timer of 20 minutes:

```
filter-c User-Password="ascend", Service-Type=Outbound-User
   Ascend-Cache-Time=20
   Ascend-Cache-Refresh=Refresh-Yes
```

```
   Ascend-Data-Filter="ip out forward tcp dstip 10.1.1.3/16"
   Ascend-Data-Filter="ip out drop"
```

See Also: "Ascend-Cache-Time (57)" on page 4-25.

Ascend-Cache-Time (57)

Description: Indicates the time (in minutes) for which the filter profile or private-route profile should remain cached.

Usage: Specify an integer. The minimum possible cache time is 0 (zero) minutes, which causes the system to retrieve the profile for every route lookup in the table. This setting is usually not desirable.

Example: The following specifies a cache time of 20 minutes for the filter profile:

```
filter-c User-Password="ascend", Service-Type=Outbound-User
   Ascend-Cache-Time=20
   Ascend-Cache-Refresh=Refresh-Yes
   Ascend-Data-Filter="ip out forward tcp dstip 10.1.1.3/16"
   Ascend-Data-Filter="ip out drop"
```

Dependencies: Consider the following:

- If you do not specify the Ascend-Cache-Time attribute in a filter or private-route profile, the profile will be cached for the amount of time specified by the local configuration of the TAOS unit.
- When the cache timer expires for a RADIUS profile, the profile is deleted from system memory. The next time the profile is needed, the system retrieves it from RADIUS and stores it in the cache again. Keeping a profile in cache increases the performance of route lookups at the cost of some system memory.

See Also: "Ascend-Cache-Refresh (56)" on page 4-24.

Ascend-Call-Attempt-Limit (123)

Description: Specifies how many unsuccessful dialout attempts can occur before the TAOS unit blocks further connection attempts.

Usage: Specify an integer. The default is 0 (zero), which disables call blocking.

Example: The following profile specifies that after the two unsuccessful attempts, the unit blocks further connection attempts:

```
prof-out User-Password="ascend" Service-Type=Outbound-User,
        User-Name="prof",
        Ascend-Dial-Number="93469699",
        Ascend-Send-Auth=Send-Auth-PAP,
        Ascend-Send-Passwd="test",
        Framed-IP-Address=200.178.179.100,
        Framed-IP-Netmask=255.255.0.0,
        Ascend-Call-Attempt-Limit=2,
        Ascend-Call-Block-Duration=15
```

See Also: "Ascend-Call-Block-Duration (124)" on page 4-27.

Ascend-Callback (246)

Description: Enables or disables callback.

Callback occurs when the TAOS unit answers a call and verifies a name and password against a user profile. If Ascend-Callback=Yes, the TAOS unit hangs up and dials back to the caller by using the following values:

- The phone number specified by Ascend-Dial-Number
- The password specified by Ascend-Send-Secret or Ascend-Send-Passwd
- Any other relevant attributes in the user profile that authenticated the call

If you set up a RADIUS user profile for callback and CLID-only authentication, the TAOS unit never answers the call. The caller therefore avoids billing charges.

Usage: Specify one of the following values:

- Callback-No (0) specifies that the TAOS unit answers in the normal manner after authentication. Callback-No is the default.
- Callback-Yes (1) specifies that the TAOS unit hangs up and calls back after authentication.

Example: In the following example, the user named Emma dials in, and the TAOS unit hangs up and calls back. When the unit calls back, it requests PAP authentication over an MP+ link. You would configure Emma's user profile as follows:

```
Emma User-Password="pwd"
     Service-Type=Framed-User,
     Ascend-Data-Svc=Switched-56K,
     Ascend-Maximum-Time=180,
     Ascend-Dial-Number=555-1213,
     Framed-Route="10.1.2.4 10.1.2.3",
     Ascend-Callback=Callback-Yes,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.1.2.3,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Passwd="test"
```

Dependencies: The Ascend-Callback attribute applies only to incoming calls and should not appear in dial-out user profiles (when Service-Type=Outbound-User).

See Also: "Ascend-Callback-Delay (108)" on page 4-26.

Ascend-Callback-Delay (108)

Description: Specifies the number of seconds the TAOS unit waits before calling back a remote user.

Usage: Specify an integer from 0 through 60. The unit treats values of 0–3 as 3 seconds. The default is 0 (zero).

Example: In the following example, the TAOS unit waits ten seconds before calling back the user Emma:

```
Emma User-Password="pwd"
     Service-Type=Framed-User,
```

```
Ascend-Data-Svc=Switched-56K,
Ascend-Maximum-Time=180,
Ascend-Dial-Number=555-1213,
Framed-Route="10.1.2.4 10.1.2.3",
Ascend-Callback=Callback-Yes,
Ascend-Callback-Delay=10,
Framed-Protocol=MPP,
Framed-IP-Address=10.1.2.3,
Ascend-Send-Auth=Send-Auth-PAP,
Ascend-Send-Passwd="test"
```

Dependencies: If Ascend-Callback=Callback-No, Ascend-Callback-Delay does not apply.

See Also: "Ascend-Callback (246)" on page 4-26.

Ascend-Call-Block-Duration (124)

Description: Specifies the period (in seconds) during which the TAOS unit refuses dialout attempts after the Ascend-Call-Attempt-Limit has been reached.

Usage: Specify an integer. The default is 0 (zero).

Example: The following profile specifies that the unit refuses dialout attempts for 15 seconds after reaching the Ascend-Call-Attempt-Limit:

```
prof-out User-Password="ascend" Service-Type=Outbound-User,
        User-Name="prof",
        Ascend-Dial-Number="93469699",
        Ascend-Send-Auth=Send-Auth-PAP,
        Ascend-Send-Passwd="test",
        Framed-IP-Address=200.178.179.100,
        Framed-IP-Netmask=255.255.0.0,
        Ascend-Call-Attempt-Limit=2,
        Ascend-Call-Block-Duration=15
```

Dependencies: For Ascend-Call-Block-Duration to apply, you must set Ascend-Call-Attempt-Limit to a nonzero value.

See Also: "Ascend-Call-Attempt-Limit (123)" on page 4-25.

Ascend-Call-By-Call (250)

Description: Specifies the T1 PRI service that the TAOS unit uses when placing a PPP, MP, or MP+ call.

Usage: Specify a number corresponding to the type of service the TAOS unit uses. The default value is 6. Table 4-3 lists the services available for each service provider.

Table 4-3. Ascend-Call-By-Call settings

Number	AT&T	Sprint	MCI
0	Disable call-by-call service.	Reserved	N/A

Table 4-3. Ascend-Call-By-Call settings (continued)

Number	AT&T	Sprint	MCI
1	SDN (including GSDN)	Private	VNET/Vision
2	Megacom 800	Inwatts	800
3	Megacom	Outwatts	PRISM1, PRISM II, WATS
4	N/A	FX	900
5	N/A	Tie Trunk	DAL
6	ACCUNET Switched Digital Services	N/A	N/A
7	Long Distance Service (including AT&T World Connect)	N/A	N/A
8	International 800 (I800)	N/A	N/A
16	AT&T MultiQuest	N/A	N/A

Example: In the following example, the pseudo-user profile is configured to initiate a call by means of AT&T long-distance service to a TAOS unit called Homer:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
     User-Name="Homer",
     Ascend-Dial-Number=1-212-555-3131,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.0.100.1,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Call-By-Call=7
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

See Also: “Ascend-PRI-Number-Type (226)” on page 4-117.

Ascend-Call-Filter (243)

Description: Specifies the characteristics of a call filter in a RADIUS user profile. The TAOS unit uses the filter only when it places a call or receives a call associated with the profile that includes the filter definition.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which you enter them is significant. If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile.

You can specify an IP filter or a generic filter. The following subsections describe how to configure each of the filter types.

IP call filter entries

Use the following format for an IP call filter entry:

```
Ascend-Call-Filter="ip dir action [dstip dest_ipaddr\subnet_mask]
[srcip src_ipaddr\subnet_mask] [proto [dstport cmp value
[srcport cmp value] [est]]"
```

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines here for printing purposes only.

Table 4-4 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-4. IP call filter syntax elements

Element	Description
`ip`	Specifies an IP filter.
`dir`	Specifies filter direction. You can specify `in` (to filter packets coming into the TAOS unit) or `out` (to filter packets going out of the TAOS unit).
`action`	Specifies the action the TAOS unit should take with a packet that matches the filter. You can specify either `forward` or `drop`.
`dstip` *`dest_ipaddr`* `\`*`subnet_mask`*	The keyword `dstip` enables destination-IP-address filtering. The filter applies to packets whose destination address matches the value of *`dest_ipaddr`*. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If you set *`dest_ipaddr`* to 0.0.0.0, or if the keyword and its IP address specification are not present, the filter matches all IP packets.
`srcip` *`src_ipaddr`* `\`*`subnet_mask`*	The keyword `srcip` enables source-IP-address filtering. The filter applies to packets whose source address matches the value of *`src_ipaddr`*. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If you set *`src_ipaddr`* to 0.0.0.0, or if the keyword and its specification are not present, the filter matches all IP packets.
`proto`	Specifies a protocol specified as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are `icmp` (1), `tcp` (6), `udp` (17), and `ospf` (89). If you set *`proto`* to 0 (zero), the filter matches any protocol.

Table 4-4. IP call filter syntax elements (continued)

Element	Description
`dstport` *`cmp value`*	The keyword `dstport` enables destination-port filtering. This argument is valid only when the protocol is `tcp` (6) or `udp` (17). If you do not specify a destination port, the filter matches any port. The *`cmp`* argument defines how to compare the specified value to the actual destination port. It can have the value `<`, `=`, `>`, or `!=`. The *`value`* argument can be a number or a name. Supported names and numbers are `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), and `talk` (517).
`srcport` *`cmp value`*	The keyword `srcport` enables source-port filtering. It is valid only when the protocol is `tcp` (6) or `udp` (17). If you do not specify a source port, the filter matches any port. The *`cmp`* argument defines how to compare the specified value to the actual source port. It can have the value `<`, `=`, `>`, or `!=`. The *`value`* argument can be a number or a name. Supported names and numbers are `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), and `talk` (517).
`est`	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the *`proto`* specification is `tcp` (6).

Generic call filter entries

Use the following format for a generic call filter entry:

`Ascend-Call-Filter="generic` *`dir action offset mask value compare`* `[more]"`

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines here for printing purposes only.

Table 4-5 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-5. Generic call filter syntax elements

Element	Description
`generic`	Specifies a generic filter.

Table 4-5. Generic call filter syntax elements (continued)

Element	Description
dir	Defines filter direction. You can specify `in` (to filter packets coming into the TAOS unit) or `out` (to filter packets going out of the TAOS unit).
action	Defines the action the TAOS unit should take with a packet that matches the filter. You can specify either `forward` or `drop`.
offset	Specifies the number of bytes masked from the start of the packet. The byte position specified by *offset* is called the byte-offset. Starting at the position specified by *offset*, the TAOS unit applies the value of the *mask* argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. The unit then compares the unmasked portion of the packet with the value specified by the *value* argument.
mask	Specifies which bits to compare in a segment of the packet. The mask must not exceed 6 bytes (12 hexadecimal digits). A one bit in the mask indicates a bit to compare. A zero bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	Specifies the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask. Otherwise, the TAOS unit ignores the filter.
compare	Defines how the TAOS unit compares a packet's contents to the value specified by *value*. You can specify `==` (for Equal) or `!=` (for NotEqual). Equal is the default.
`more`	If present, specifies whether the TAOS unit applies the next filter definition in the profile to the current packet before deciding whether to forward or drop the packet. The *dir* and *action* values for the next entry must be the same as the *dir* and *action* values for the current entry. Otherwise, the TAOS unit ignores the `more` flag.

Example: The following are examples of IP call filter entries:

```
Ascend-Call-Filter="ip in drop"

Ascend-Call-Filter="ip out forward tcp"

Ascend-Call-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 dstport!=telnet"

Ascend-Call-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 icmp"
```

The following are examples of generic call filter entries:

```
Ascend-Call-Filter="generic in drop 0 ffff 0080"

Ascend-Call-Filter="generic in drop 0 ffff != 0080 more"
```

```
Ascend-Call-Filter="generic in drop 16 ff aa"
```

See Also: "Ascend-Data-Filter (242)" on page 4-45.

Ascend-Calling-Id-Numbering-Plan (67)

Description: Specifies the NumberPlanID field in the calling party's information element.

Usage: Ask your provider about which of the following settings to specify:

- Unknown (0) specifies NumberPlanID=0. The network has no knowledge of the numbering plan.
- ISDN-Telephony (1) specifies NumberPlanID=1, and follows recommendation E.164.
- Data (3) specifies NumberPlanID=3, and follows recommendation X.121.
- Telex (4) specifies NumberPlanID=4, and follows recommendation F.69.
- National (8) specifies NumberPlanID=8, the national standard numbering plan.
- Private (9) specifies NumberPlanID=9, a private numbering plan.

Example: The following user profile specifies CLID authentication with a name, password, and caller ID, and requires that NumberPlanID=3:

```
Emma  User-Password="test", Calling-Station-Id="123456789"
      Ascend-Calling-Id-Numbering-Plan=Data,
      Ascend-Calling-Id-Presentation=Restricted,
      Ascend-Calling-Id-Screening=User-Provided-Passed,
      Ascend-Calling-Id-Type-Of-Number=National-Number,
      Service-Type=Framed-User,
      Framed-Protocol=PPP,
      Framed-IP-Address=255.255.255.254,
      Framed-IP-Netmask=255.255.255.255,
      Ascend-Route-IP=Route-IP-Yes
```

Dependencies: Ascend-Calling-Id-Numbering-Plan appears in an Access-Request packet.

See Also: "Ascend-Calling-Id-Presentation (68)" on page 4-32,
"Ascend-Calling-Id-Screening (69)" on page 4-33, and
"Ascend-Calling-Id-Type-Of-Number (66)" on page 4-34.

Ascend-Calling-Id-Presentation (68)

Description: Specifies whether the calling-party number is confidential.

Usage: Specify one of the following values:

- Allowed (0) specifies that the calling-party number can be made available outside the network.
- Restricted (1) specifies that the calling-party number is confidential and restricted to network use only.
- Number-Not-Available (2) specifies that the telephone network attempted to obtain the calling-party number but was unable to do so.

Example: The following user profile specifies CLID authentication with a name, password, and caller ID, and requires that the calling-party number be restricted to network use only:

```
Emma  User-Password="test", Calling-Station-Id="123456789"
      Ascend-Calling-Id-Numbering-Plan=Data,
      Ascend-Calling-Id-Presentation=Restricted,
      Ascend-Calling-Id-Screening=User-Provided-Passed,
      Ascend-Calling-Id-Type-Of-Number=National-Number,
      Service-Type=Framed-User,
      Framed-Protocol=PPP,
      Framed-IP-Address=255.255.255.254,
      Framed-IP-Netmask=255.255.255.255,
      Ascend-Route-IP=Route-IP-Yes
```

Dependencies: Ascend-Calling-Id-Presentation appears in an Access-Request packet.

See Also: "Ascend-Calling-Id-Numbering-Plan (67)" on page 4-32, "Ascend-Calling-Id-Screening (69)" on page 4-33, and "Ascend-Calling-Id-Type-Of-Number (66)" on page 4-34.

Ascend-Calling-Id-Screening (69)

Description: Specifies the origin of the calling-party ID.

Usage: Specify one of the following values:

- User-Not-Screened (0) specifies the calling number was provided by the user and was not screened. The origin of the calling-party ID cannot be verified.
- User-Provided-Passed (1) specifies that the user provided the calling-party ID and passed the screening criteria.
- User-Provided-Failed (2) specifies that the user provided the calling-party ID, but failed the screening criteria.
- Network-Provided (3) specifies that the network originated the calling-party ID.

Example: The following user profile specifies CLID authentication with a name, password, and caller ID, and requires that the user provide the calling-party ID and pass the screening criteria:

```
Emma  User-Password="test", Calling-Station-Id="123456789"
      Ascend-Calling-Id-Numbering-Plan=Data,
      Ascend-Calling-Id-Presentation=Restricted,
      Ascend-Calling-Id-Screening=User-Provided-Passed,
      Ascend-Calling-Id-Type-Of-Number=National-Number,
      Service-Type=Framed-User,
      Framed-Protocol=PPP,
      Framed-IP-Address=255.255.255.254,
      Framed-IP-Netmask=255.255.255.255,
      Ascend-Route-IP=Route-IP-Yes
```

Dependencies: Ascend-Calling-Id-Screening appears in an Access-Request packet.

See Also: "Ascend-Calling-Id-Presentation (68)" on page 4-32, "Ascend-Calling-Id-Screening (69)" on page 4-33, and "Ascend-Calling-Id-Type-Of-Number (66)" on page 4-34.

Ascend-Calling-Id-Type-Of-Number (66)

Description: Specifies the type of phone number used by the caller.

Usage: Specify one of the following values:

- Unknown (0) specifies that the phone number is of an unknown type. The number might include a prefix or escape digits.
- International-Number (1) specifies a phone number outside the U.S. The number does not include a prefix or escape digits.
- National-Number (2) specifies a phone number within the U.S. The number does not include a prefix or escape digits.
- Network-Specific (3) specifies that the dialed network interprets the phone number. This setting uses TypeOfNumber=3 in the called party's Information Element.
- Subscriber-Number (4) specifies a phone number within your Centrex group. The number does not include a prefix or escape digits.
- Abbreviated-Number (6) specifies add-on numbers only.

Example: The following profile requires that the user call from a number inside the U.S. CLID authentication with a name, password, and caller ID must also take place:

```
Emma  User-Password="test", Calling-Station-Id="123456789"
      Ascend-Calling-Id-Numbering-Plan=Data,
      Ascend-Calling-Id-Presentation=Restricted,
      Ascend-Calling-Id-Screening=User-Provided-Passed,
      Ascend-Calling-Id-Type-Of-Number=National-Number,
      Service-Type=Framed-User,
      Framed-Protocol=PPP,
      Framed-IP-Address=255.255.255.254,
      Framed-IP-Netmask=255.255.255.255,
      Ascend-Route-IP=Route-IP-Yes
```

Dependencies: Ascend-Calling-Id-Type-Of-Number appears in an Access-Request packet.

See Also: "Ascend-Calling-Id-Numbering-Plan (67)" on page 4-32, "Ascend-Calling-Id-Presentation (68)" on page 4-32, and "Ascend-Calling-Id-Screening (69)" on page 4-33.

Ascend-Calling-Subaddress (107)

Description: Specifies the ISDN subaddress that the TAOS unit sends to RADIUS during Calling-Line ID (CLID) authentication.

Usage: Specify a subaddress.

Example: In the following example, the ISDN subaddress is specified on the first line of the profile:

```
ace5 User-Password="pizza", Calling-Station-Id="1110963207",
Ascend-Calling-Subaddress="12345"
     Service-Type=Framed-User,
     Framed-Protocol=PPP,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Route-IP =Route-IP-No,
```

```
Ascend-Base-Channel-Count=1,
Ascend-Minimum-Channels=1,
Ascend-Maximum-Channels=2
```

Dependencies: Ascend-Calling-Subaddress appears in Access-Request and Accounting Start packets.

See Also: "Calling-Station-Id (31)" on page 4-145.

Ascend-Call-Type (177)

Description: Specifies the type of nailed-up connection in use.

Usage: Table 4-6 lists the settings you can specify for Ascend-Call-Type.

Table 4-6. Ascend-Call-Type settings

Setting	Specifies
Switched (0)	Link that consists entirely of switched channels.
Nailed (1)	Link that consists entirely of nailed-up channels. Nailed is the default.
Nailed/Mpp (2)	Link that consists of both nailed-up and switched channels. The TAOS unit establishes the connection whenever any of its nailed-up or switched channels are connected end-to-end. If a Nailed/Mpp link is down and the nailed-up channels are down, the link cannot reestablish itself until the TAOS unit brings up one or more of the nailed-up channels, or dials one or more switched channels. Typically, the TAOS unit dials the switched channels when it receives a packet whose destination is the unit at the remote end of the Nailed/Mpp connection. The packet initiating the switched call must come from the caller side of the connection. If a failed channel is in the group specified by the Ascend-Group attribute, the TAOS unit replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels. The TAOS unit always replaces failed nailed-up channels with switched channels, regardless of the Ascend-Minimum-Channels setting.

Table 4-6. Ascend-Call-Type settings (continued)

Setting	Specifies
Perm/Switched (3)	Permanent switched connection (an outbound call that the TAOS unit attempts to keep up at all times). If the unit or central switch resets, or if one end terminates the link, the permanent switched connection attempts to restore the link at 10-second intervals. Use this setting if your telephone company charges for each incoming and outgoing connection attempt, but does not charge for connection time on local calls. Lucent's regular bandwidth-on-demand feature conserves connection time but causes many connection attempts. A permanent switched connection performs the opposite function. It conserves connection attempts but causes a long connection time. For the answering device at the remote end of the permanent switched connection, Lucent recommends that you configure the Connection profile to answer calls but not originate them. If the remote device initiates a call, the TAOS unit simply does not answer it. This situation could result in repeated charges for calls that have no purpose. To keep the remote device from originating calls, set Answer-Originate=Ans-Only for that device.
AO/DI (6)	Always On/Dynamic ISDN (AO/DI) session. AO/DI is a networking service that enables you to send and receive data through a nailed-up X.25 connection over an ISDN D channel, ISDN B channel, or nailed-up 56K line.
MegaMax (7)	MegaMax MP+ session. Each call in a MegaMax MP+ session can use a different number of H0 and H11 channels than other calls in the session.

Example: The following pseudo-user profile specifies a Nailed/MPP connection:

```
permconn-Alameda-1 User-Password="ascend", Service-Type=Outbound-User
       User-Name="CA",
       Framed-Protocol=MPP,
       Framed-IP-Address=50.1.1.1,
       Framed-IP-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Call-Type=Nailed/Mpp,
       Ascend-Group="1,3,5,7",
       Ascend-FT1-Caller=FT1-Yes,
       Ascend-Target-Util=80,
       Ascend-History-Weigh-Type=History-Constant,
       Ascend-Seconds-Of-History=90,
       Ascend-Add-Seconds=30,
       Ascend-Remove-Seconds=30,
       Ascend-Maximum-Channels=10,
       Ascend-Inc-Channel-Count=2,
```

```
Ascend-Dec-Channel-Count=2,
Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: The TAOS unit adds or subtracts switched channels on a Nailed/Mpp connection as the settings on either side of the connection require. Each side makes its calculations on the basis of the traffic it receives at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.

Ascend-CBCP-Enable (112)

Description: Specifies how the TAOS unit responds to requests by callers to support CBCP.

Usage: Specify one of the following settings:

- CBCP-Not-Enabled (0) specifies that the TAOS unit rejects any request to support CBCP.
- CBCP-Enabled (1) specifies that during LCP negotiations the TAOS unit acknowledges support for CBCP.

Example: The following user profile specifies that the TAOS unit supports CBCP for the connection:

```
Jim User-Password="mypw", Service-Type=Framed-User
        Framed-Protocol=PPP,
        Ascend-Dial-Number="555-5555",
        Ascend-Data-Svc=Switched-Modem,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-CBCP-Enable=CBCP-Enabled,
        Ascend-CBCP-Mode=CBCP-Profile-Callback,
        Ascend-CBCP-Trunk-Group=5,
        Ascend-Route-IP=Route-IP-Yes,
        Ascend-Assign-IP-Pool=5
```

See Also: "Ascend-CBCP-Mode (113)" on page 4-37 and "Ascend-CBCP-Trunk-Group (115)" on page 4-38.

Ascend-CBCP-Mode (113)

Description: Specifies the method of callback the TAOS unit offers the incoming caller.

Usage: Specify one of the following values:

- CBCP-No-Callback (1) specifies that no callback method is offered. This setting applies to Windows NT or Windows 95 clients who must not be called back. Because CBCP has been negotiated initially, the Windows clients must have validation from the TAOS unit that no callback is used for the connection.
- CBCP-User-Callback (2) specifies that the caller supplies the number that the TAOS unit uses for the callback.
- CBCP-Profile-Callback (3) specifies that the TAOS unit uses the number specified by Ascend-Dial-Number for the callback.
- CBCP-User-Or-No (7) specifies that the caller has the option of supplying the number or specifying that no callback is used for the call. If no callback takes place, the call will not be disconnected by the TAOS unit.

Example: The following user profile specifies that the TAOS unit uses the number 555-5555 for the callback:

```
Jim User-Password="mypw", Service-Type=Framed-User
        Framed-Protocol=PPP,
        Ascend-Dial-Number="555-5555",
        Ascend-Data-Svc=Switched-Modem,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-CBCP-Enable=CBCP-Enabled,
        Ascend-CBCP-Mode=CBCP-Profile-Callback,
        Ascend-CBCP-Trunk-Group=5,
        Ascend-Route-IP=Route-IP-Yes,
        Ascend-Assign-IP-Pool=5
```

Dependencies: Ascend-CBCP-Mode applies only if CBCP is successfully negotiated for a connection.

See Also: "Ascend-CBCP-Enable (112)" on page 4-37 and "Ascend-CBCP-Trunk-Group (115)" on page 4-38.

Ascend-CBCP-Trunk-Group (115)

Description: Assigns the callback or outgoing IP-Fax call to a trunk group. The value in Ascend-CBCP-Trunk-Group is prepended to the number that the TAOS dials for callback or outgoing fax.

Usage: Specify a trunk-group number from 1 to 9.

Example: The following user profile specifies that the TAOS unit uses the number 555-5555 on trunk group 5 for the callback:

```
Jim User-Password="mypw", Service-Type=Framed-User
        Framed-Protocol=PPP,
        Ascend-Dial-Number="555-5555",
        Ascend-Data-Svc=Switched-Modem,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-CBCP-Enable=CBCP-Enabled,
        Ascend-CBCP-Mode=CBCP-Profile-Callback,
        Ascend-CBCP-Trunk-Group=5,
        Ascend-Route-IP=Route-IP-Yes,
        Ascend-Assign-IP-Pool=5
```

Dependencies: Ascend-CBCP-Trunk-Group applies only if one or both of the following conditions are true:

- Callback Control Protocol (CBCP) is negotiated for a connection.
- The call is an outgoing IP-Fax call and trunk groups are enabled.

See Also: "Ascend-CBCP-Enable (112)" on page 4-37 and "Ascend-CBCP-Mode (113)" on page 4-37.

Ascend-Ckt-Type (16)

Description: Specifies whether the Frame Relay circuit is a Permanent Virtual Circuit (PVC) or a Switched Permanent Circuit (SVC).

Usage: Specify one of the following values:

- Ascend-PVC specifies that the Frame Relay circuit is a PVC.
- Ascend-SVC specifies that the Frame Relay circuit is an SVC.

Example: In the following example, the profile specifies that the Frame Relay circuit is a PVC:

```
permconn-unit-1 User-Password="ascend", Service-Type=Outbound-User
   User-Name="EndPoint1",
   Ascend-FR-Profile-Name="FR Prof 1",
   Ascend-FR-DLCI=16,
   Ascend-FR-Circuit-Name="Circuit1",
   Framed-Protocol=FR-CIR,
   Ascend-Ckt-Type-Ascend-PVC
```

See Also: "Ascend-FR-Circuit-Name (156)" on page 4-76 and "Ascend-SVC-Enabled (17)" on page 4-134.

Ascend-Client-Assign-DNS (137)

Description: Specifies whether or not the TAOS unit sends the Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS values during connection negotiation.

Usage: Specify one of the following settings:

- DNS-Assign-No (0) disables client DNS server negotiation for the link. DNS-Assign-No is the default.
- DNS-Assign-Yes (1) enables client DNS server negotiation for the link.

Example: To specify that the user Emma can access two DNS servers, you would configure her user profile as follows:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=11.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Client-Assign-DNS=DNS-Assign-Yes,
     Ascend-Client-Primary-DNS=10.8.9.20
     Ascend-Client-Secondary-DNS=10.8.9.21
```

Dependencies: To direct the TAOS unit to send the client DNS server address during connection negotiation, you must include the setting Ascend-Client-Assign-DNS=DNS-Assign-Yes, and specify a valid DNS server by means of the Ascend-Client-Primary-DNS or Ascend-Client-Secondary-DNS attribute.

See Also: "Ascend-Client-Primary-DNS (135)" on page 4-40 and "Ascend-Client-Secondary-DNS (136)" on page 4-41.

Ascend-Client-Assign-WINS (80)

Description: Specifies whether the TAOSunit presents Windows Internet Name Service (WINS) server addresses to the dial-in client while negotiating the session.

Usage: Specify one of the following settings:

- WINS-Assign-No (0) specifies that the unit does not present Windows Internet Name Service (WINS) server addresses to the dial-in client.
- WINS-Assign-Yes (1) specifies that the unit presents Windows Internet Name Service (WINS) server addresses to the dial-in client.

Example: To specify that the user Carla can access two WINS servers, you would configure her user profile as follows:

```
Carla User-Password="mypw", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.10,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Client-Assign-WINS=WINS-Assign-Yes,
      Ascend-Client-Primary-WINS=10.8.9.20
      Ascend-Client-Secondary-WINS=10.8.9.21
```

Dependencies: Consider the following:

- For the client WINS feature to work, the PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings.
- You must specify the IP address of a WINS server by means of the Ascend-Client-Primary-WINS attribute.

See Also: "Ascend-Client-Primary-WINS (78)" on page 4-41 and "Ascend-Client-Secondary-WINS (79)" on page 4-42.

Ascend-Client-Primary-DNS (135)

Description: Specifies a primary DNS server address to send to any client connecting to the TAOS unit.

Usage: Specify the IP address of the primary DNS server. You must specify the address in dotted decimal notation. The default is 0.0.0.0, which specifies that no primary DNS server is available for the connection. If you do not specify Ascend-Client-Primary-DNS or Ascend-Client-Secondary-DNS in any user profile, the TAOS unit routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

Example: To specify that the user Emma can access the primary DNS server at IP address 10.8.9.20, you would configure her user profile as follows:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=11.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Client-Assign-DNS=DNS-Assign-Yes,
     Ascend-Client-Primary-DNS=10.8.9.20
     Ascend-Client-Secondary-DNS=10.8.9.21
```

Dependencies: You must include the setting Ascend-Client-Assign-DNS=DNS-Assign-Yes to direct the TAOS unit to send the primary DNS server address during connection negotiation.

See Also: "Ascend-Client-Assign-DNS (137)" on page 4-39 and
"Ascend-Client-Secondary-DNS (136)" on page 4-41.

Ascend-Client-Primary-WINS (78)

Description: Specifies the primary Windows Internet Name Service (WINS) server IP address. The primary server will be used for WINS name resolution. The secondary server, if one is specified, is used only if the primary server is unavailable.

Usage: Specify the IP address of a WINS server.

Example: To specify that the user Carla can access the primary WINS server at IP address 10.8.9.20, you would configure her user profile as follows:

```
Carla User-Password="mypw", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.10,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Client-Assign-WINS=WINS-Assign-Yes,
      Ascend-Client-Primary-WINS=10.8.9.20
      Ascend-Client-Secondary-WINS=10.8.9.21
```

Dependencies: Consider the following:

- For the client WINS feature to work, the PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings.
- For the system to pass the server address to the dial-in client during session negotiation, Ascend-Client-Assign-WINS must be set to WINS-Assign-Yes.

See Also: "Ascend-Client-Assign-WINS (80)" on page 4-39 and
"Ascend-Client-Secondary-WINS (79)" on page 4-42.

Ascend-Client-Secondary-DNS (136)

Description: Specifies a secondary DNS server address to send to any client connecting to the TAOS unit.

Usage: Specify the IP address of the secondary DNS server. You must specify the address in dotted decimal notation. The default is 0.0.0.0, which specifies that no primary DNS server is available for the connection. If you do not specify Ascend-Client-Primary-DNS or Ascend-Client-Secondary-DNS in any user profile, the TAOS unit routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

Example: To specify that the user Emma can access the secondary DNS server at IP address 10.8.9.21, you would configure her user profile as follows:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=11.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Client-Assign-DNS=DNS-Assign-Yes,
     Ascend-Client-Primary-DNS=10.8.9.20
     Ascend-Client-Secondary-DNS=10.8.9.21
```

Dependencies: You must include the setting Ascend-Client-Assign-DNS=DNS-Assign-Yes to direct the TAOS unit to send the secondary DNS server address during connection negotiation.

See Also: "Ascend-Client-Assign-DNS (137)" on page 4-39 and "Ascend-Client-Primary-DNS (135)" on page 4-40.

Ascend-Client-Secondary-WINS (79)

Description: Specifies the secondary Windows Internet Name Service (WINS) server IP address. The TAOS unit uses the secondary server for WINS name resolution only if the primary server is unavailable.

Usage: Specify the IP address of a WINS server.

Example: To specify that the user Carla can access the secondary WINS server at IP address 10.8.9.21, you would configure her user profile as follows:

```
Carla User-Password="mypw", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.10,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Client-Assign-WINS=WINS-Assign-Yes,
      Ascend-Client-Primary-WINS=10.8.9.20
      Ascend-Client-Secondary-WINS=10.8.9.21
```

Dependencies: Consider the following:

- For the client WINS feature to work, the PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings.
- For the system to pass the server address to the dial-in client during session negotiation, Ascend-Client-Assign-WINS must be set to WINS-Assign-Yes.

See Also: "Ascend-Client-Assign-WINS (80)" on page 4-39 and "Ascend-Client-Primary-WINS (78)" on page 4-41.

Ascend-Connect-Progress (196)

Description: Indicates the state of the connection before it disconnects.

Usage: When a call disconnects, the TAOS unit typically sends the following message:

`call` *`n`* `CL OK u=` *`username`* `c=`*`n`* `p=`*`m`*

where:

- *`n`* specifies a disconnect code that indicates why the call disconnected.
- *`m`* specifies a progress code that indicates how far the call had progressed when it disconnected.

Table 4-7 provides a list of progress codes and their meanings.

Table 4-7. Progress codes

Code	Explanation
1	Not applied to any call.
2	Unknown progress.
7	Call still connecting.
10	TAOS unit has detected and accepted the call.
11	Dialed service was blocked.
30	TAOS unit has assigned a modem to the call.
31	Modem is awaiting DCD from the remote modem.
32	Modem is awaiting result codes from the remote modem.
40	Terminal-server session started.
41	Raw TCP session started.
42	Immediate Telnet session started.
43	Connection made to a raw TCP host.
44	Connection made to a Telnet host.
45	Rlogin session started.
46	Connection made with an Rlogin session.
47	Terminal-server authentication started.
50	Modem outdial session started.
60	LAN session is up.
61	Opening LCP.
62	Opening CCP.
63	Opening IPNCP.
64	Opening BNCP.
65	LCP opened.
66	CCP opened.
67	IPNCP opened.
68	BNCP opened.

Table 4-7. Progress codes (continued)

Code	Explanation
69	LCP is in Initial state.
70	LCP is in Starting state.
71	LCP is in Closed state.
72	LCP is in Stopped state.
73	LCP is in Closing state.
74	LCP is in Stopping state.
75	LCP is in Req-Sent state.
76	LCP is in Ack-Rcvd state.
77	LCP is in Ack-Sent state.
80	IPX NCP is in Open state.
81	AT NCP is in Open state.
82	BACP is being opened.
83	BACP is now open.
84	CBCP is being opened.
85	CBCP is now open.
90	TAOS has accepted a V.110 call.
91	V.110 call is in Opened state.
92	V.110 call is in Carrier state.
93	V.110 call is in Reset state.
94	V.110 call is in Closed state.
100	TAOS unit determines that the call requires callback.
101	Authentication failed.
102	Remote authentication server timed out.
120	Frame Relay link is inactive. Negotiations are in progress.
121	Frame Relay link is active and has end-to-end connectivity.
200	Starting Authentication layer.

Table 4-7. Progress codes (continued)

Code	Explanation
201	Authentication layer moving to opening state.
202	Skipping Authentication layer.
203	Authentication layer is in opened state.

Dependencies: The TAOS unit includes Ascend-Connect-Progress in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

See Also: "Ascend-Disconnect-Cause (195)" on page 4-57.

Ascend-Data-Filter (242)

Description: Specifies the characteristics of a data filter in a RADIUS user profile or pseudo-user profile.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which you enter them is significant. If you make changes to a filter, the changes do not take effect until a call uses that profile.

You can specify an IP filter or a generic filter. The following sections describe how to configure each of the filter types.

IP data filter entries

Use the following format for an IP data filter entry:

```
Ascend-Data-Filter="ip dir action [dstip dest_ipaddr\subnet_mask]
[srcip src_ipaddr\subnet_mask] [proto [dstport cmp value
[srcport cmp value] [est]]"
```

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines here for printing purposes only.

Table 4-8 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-8. IP data filter syntax elements

Element	Description7
`ip`	Specifies an IP filter.
`dir`	Specifies filter direction. You can specify `in` (to filter packets coming into the TAOS unit) or `out` (to filter packets going out of the TAOS unit).
`action`	Specifies the action the TAOS unit should take with a packet that matches the filter. You can specify either `forward` or `drop`.

Table 4-8. IP data filter syntax elements (continued)

Element	Description7
`dstip` *`dest_ipaddr \subnet_mask`*	The keyword `dstip` enables destination-IP-address filtering. The filter applies to packets whose destination address matches the value of *`dest_ipaddr`*. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If you set *`dest_ipaddr`* to 0.0.0.0, or if the keyword and its IP address specification are not present, the filter matches all IP packets.
`srcip` *`src_ipaddr \subnet_mask`*	The keyword `srcip` enables source-IP-address filtering. The filter applies to packets whose source address matches the value of *`src_ipaddr`*. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If you set *`src_ipaddr`* to 0.0.0.0, or if the keyword and its specification are not present, the filter matches all IP packets.
`proto`	Specifies a protocol specified as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are `icmp` (1), `tcp` (6), `udp` (17), and `ospf` (89). If you set *`proto`* to 0 (zero), the filter matches any protocol.
`dstport` *`cmp value`*	The keyword `dstport` enables destination-port filtering. This argument is valid only when the protocol is `tcp` (6) or `udp` (17). If you do not specify a destination port, the filter matches any port. The *`cmp`* argument defines how to compare the specified value to the actual destination port. It can have the value `<`, `=`, `>`, or `!=`. The *`value`* argument can be a number or a name. Supported names and numbers are `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), and `talk` (517).

Table 4-8. IP data filter syntax elements (continued)

Element	Description7
`srcport` *`cmp value`*	The keyword `srcport` enables source-port filtering. It is valid only when the protocol is `tcp` (6) or `udp` (17). If you do not specify a source port, the filter matches any port. The *`cmp`* argument defines how to compare the specified value to the actual source port. It can have the value `<`, `=`, `>`, or `!=`. The *`value`* argument can be a number or a name. Supported names and numbers are `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), and `talk` (517).
`est`	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the *`proto`* specification is `tcp` (6).

Generic data filter entries

Use the following format for a generic data filter entry:

`Ascend-Data-Filter="generic` *`dir action offset mask value compare`* `[more]"`

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines here for printing purposes only.

Table 4-9 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-9. Generic data filter syntax elements

Element	Description
`generic`	Specifies a generic filter.
`dir`	Defines filter direction. You can specify `in` (to filter packets coming into the TAOS unit) or `out` (to filter packets going out of the TAOS unit).
`action`	Defines the action the TAOS unit should take with a packet that matches the filter. You can specify either `forward` or `drop`.

Table 4-9. Generic data filter syntax elements (continued)

Element	Description
offset	Specifies the number of bytes masked from the start of the packet. The byte position specified by *offset* is called the byte-offset. Starting at the position specified by *offset*, the TAOS unit applies the value of the *mask* argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. The unit then compares the unmasked portion of the packet with the value specified by the *value* argument.
mask	Specifies which bits to compare in a segment of the packet. The mask must not exceed 6 bytes (12 hexadecimal digits). A one bit in the mask indicates a bit to compare. A zero bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	Specifies the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask. Otherwise, the TAOS unit ignores the filter.
compare	Defines how the TAOS unit compares a packet's contents to the value specified by *value*. You can specify == (for Equal) or != (for NotEqual). Equal is the default.
more	If present, specifies whether the TAOS unit applies the next filter definition in the profile to the current packet before deciding whether to forward or drop the packet. The *dir* and *action* values for the next entry must be the same as the *dir* and *action* values for the current entry. Otherwise, the TAOS unit ignores the more flag.

Example: The following are examples of IP data filter entries:

```
Ascend-Data-Filter="ip in drop"
```

```
Ascend-Data-Filter="ip out forward tcp"
```

```
Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 dstport!=telnet"
```

```
Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 icmp"
```

The following are examples of generic data filter entries:

```
Ascend-Data-Filter="generic in drop 0 ffff 0080"
```

```
Ascend-Data-Filter="generic in drop 0 ffff != 0080 more"
```

```
Ascend-Data-Filter="generic in drop 16 ff aa"
```

Following is a sample RADIUS filter profile:

```
filter-c User-Password="ascend", Service-Type=Outbound
   Ascend-Cache-Time=20,
```

```
Ascend-Cache-Refresh=Refresh-Yes,
Ascend-Data-Filter="ip out forward tcp dstip 10.1.1.3/16",
Ascend-Data-Filter="ip out drop"
```

The cache timer has been set to 20 minutes, and the timer is reset each time the filter is applied to a session.

See Also: "Ascend-Call-Filter (243)" on page 4-28.

Ascend-Data-Rate (197)

Description: Specifies the receive rate of the connection in bits per second.

Usage: Ascend-Data-Rate does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-Data-Rate=31200`

Dependencies: The TAOS unit includes Ascend-Data-Rate in an Accounting-Request packet when the session has ended or has failed to authenticate (Acct-Status-Type=Stop). The TAOS unit also includes Ascend-Data-Rate in an Access-Request packet unless you authenticate with Calling-Line ID (CLID) or Dialed Number Information Service (DNIS).

See Also: "Ascend-Xmit-Rate (255)" on page 4-144.

Ascend-Data-Svc (247)

Description: Specifies the type of data service the link uses for outgoing calls.

Usage: Set the Ascend-Data-Svc attribute to one of the values listed in Table 4-10. The data service you specify must be available end-to-end.

Table 4-10. Ascend-Data-Svc settings

Setting	Description
Switched-Voice-Bearer (0)	Applies only to calls made over a T1 PRI line. The TAOS unit enables the network to place an end-to-end digital voice call for transporting data when a switched data service is not available.
Switched-56KR (1)	Contains restricted data, guaranteeing that the data the TAOS unit transmits meets the density restrictions of D4-framed T1 lines. D4 specifies the D4 format, also known as the Superframe format, for framing data at the physical layer. This format consists of 12 consecutive frames separated by framing bits. The call connects to the Switched-56 data service. The only services available to lines that use inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched-56KR.
Switched-64K (2)	Contains any type of data and connects to the Switched-64 data service.
Switched-64KR (3)	Contains restricted data and connects to the Switched-64 data service.

Table 4-10. Ascend-Data-Svc settings (continued)

Setting	Description
Switched-56K (4)	Contains any type of data and connects to the Switched-56 data service. The only services available to lines that use inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched- 56KR. For most T1 PRI lines, select Switched-56K.
Nailed-56KR (1)	Contains restricted data and connects to the Nailed-56 data service.
Nailed-64K (2)	Contains any type of data and connects to the Nailed-64 data service.
Switched-384KR (5)	Contains restricted data, and connects to MultiRate or GloBanD data services at 384 Kbps.
Switched-384K (6)	Contains any type of data and connects to the Switched-384 data service. This AT&T data service does not require MultiRate or GloBanD.
Switched-1536K (7)	Contains any type of data and connects to the Switched-1536 data service at 1536 Kbps. This setting is valid only for a TAOS unit that supports ISDN D-channel signaling, and connects to two or more T1 PRI lines that use Non-Facility Associated Signaling (NFAS).
Switched-1536KR (8)	Contains restricted data, and connects to the Switched-1536 data service at 1536 Kbps. This setting is valid only for a TAOS unit that supports ISDN D-channel signaling, and is connected to two or more T1 PRI lines that use Non-Facility Associated Signaling (NFAS).
Switched-128K (9)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-192K (10)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-256K (11)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-320K (12)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-384K-MR (13)	Available on a T1 PRI line with the MultiRate data service.
Switched-448K (14)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-512K (15)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-576K (16)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-640K (17)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-704K (18)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-768K (19)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-832K (20)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-896K (21)	Available on a T1 PRI line with MultiRate or GloBanD data services.

Table 4-10. Ascend-Data-Svc settings (continued)

Setting	Description
Switched-960K (22)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1024K (23)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1088K (24)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1152K (25)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1216K (26)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1280K (27)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1344K (28)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1408K (29)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1472K (30)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1600K (31)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1664K (32)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1728K (33)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1792K (34)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1856K (35)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1920K (36)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-inherited (37)	Specifies calls placed by a device connected to a local ISDN BRI line supplied by a Host/BRI module. The call connects with the data service as requested by the caller on the local ISDN BRI line.
Switched-restricted-bearer-x30 (38)	Specifies 56-Kbps X.30 switched service from DPNSS and DASS 2 switches.
Switched-clear-bearer-v110 (39)	Specifies the 64-kbps V.110 switched data service available from DPNSS and DASS 2 switches.
Switched-restricted-64-x30 (40)	Specifies 64-Kbps X.30 switched service from DPNSS and DASS 2 switches. For most DASS 2 and DPNSS installations, select Switched-restricted-64-x30.
Switched-clear-56-v110 (41)	Specifies the 56-kbps V.110 switched data service available from DPNSS and DASS 2 switches.
Switched-modem (42)	Places an outgoing call on any available digital modem. If no digital modems are available, the TAOS unit does not place the call. The data rate depends on the quality of the connections between modems and the types of modems used. The Switched-modem setting requires that your TAOS unit have digital modems installed. The setting applies only for PPP and MP+ calls. Currently, the TAOS unit does not support multichannel modem calls.
Switched-atmodem (43)	Equivalent to Switched-modem.

Table 4-10. Ascend-Data-Svc settings (continued)

Setting	Description
Switched-V110-24-56 (45)	Specifies a V.110 connection at 2400 baud on a 56K line.
Switched-V110-48-56 (46)	Specifies a V.110 connection at 4800 baud on a 56K line.
Switched-V110-96-56 (47)	Specifies a V.110 connection at 9600 baud on a 56K line.
Switched-V110-192-56 (48)	Specifies a V.110 connection at 19200 baud on a 56K line.
Switched-V110-384-56 (49)	Specifies a V.110 connection at 38400 baud on a 56K line.
Switched-V110-24-56R (50)	Specifies a V.110 connection with restricted data at 2400 baud on a 56K line.
Switched-V110-48-56R (51)	Specifies a V.110 connection with restricted data at 4800 baud on a 56K line.
Switched-V110-96-56R (52)	Specifies a V.110 connection with restricted data at 9600 baud on a 56K line.
Switched-V110-192-56R (53)	Specifies a V.110 connection with restricted data at 19200 baud on a 56K line.
Switched-V110-384-56R (54)	Specifies a V.110 connection with restricted data at 38400 baud on a 56K line.
Switched-V110-24-64 (55)	Specifies a V.110 connection at 2400 baud on a 64K line.
Switched-V110-48-64 (56)	Specifies a V.110 connection at 4800 baud on a 64K line.
Switched-V110-96-64 (57)	Specifies a V.110 connection at 9600 baud on a 64K line.
Switched-V110-192-64 (58)	Specifies a V.110 connection at 19200 baud on a 64K line.
Switched-V110-384-64 (59)	Specifies a V.110 connection at 38400 baud on a 64K line.
Switched-V110-24-64R (60)	Specifies a V.110 connection with restricted data at 2400 baud on a 64K line.
Switched-V110-48-64R (61)	Specifies a V.110 connection with restricted data at 4800 baud on a 64K line.
Switched-V110-96-64R (62)	Specifies a V.110 connection with restricted data at 9600 baud on a 64K line.
Switched-V110-192-64R (63)	Specifies a V.110 connection with restricted data at 19200 baud on a 64K line.
Switched-V110-384-64R (64)	Specifies a V.110 connection with restricted data at 38400 baud on a 64K line.
Switched-POTS (68)	Specifies a switched call originating from, or destined for, a Plain Old Telephone Service (POTS) port.
Switched-ATM (69)	Specifies an Asynchronous Transfer Mode (ATM) Switched Virtual Circuit (SVC).
Switched-FR (70)	Specifies a Frame Relay SVC.

Example: In the following example, the pseudo-user profile is configured to initiate a call to a TAOS unit named Homer by means of the Switched-64K data service:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
     User-Name="Homer",
     Ascend-Dial-Number=555-3131,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.0.100.1,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Data-Svc=Switched-64K,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

Dependencies: Consider the following:

- You can determine the base bandwidth of a call by multiplying the value of the Ascend-Base-Channel-Count attribute by the value of the Ascend-Data-Svc attribute.
- Either party can request a data service that is unavailable. In such a case, the TAOS unit cannot connect the call.

See Also: "Ascend-Call-Type (177)" on page 4-35.

Ascend-DBA-Monitor (171)

Description: Specifies how the TAOS calling unit monitors the traffic on an MP+ call. The TAOS unit can use the information to add or subtract bandwidth as necessary.

Usage: Specify one of the following values:

- DBA-Transmit (0) specifies that the TAOS unit adds or subtracts bandwidth on the basis of the amount of data it transmits. DBA-Transmit is the default.
- DBA-Transmit-Recv (1) specifies that the TAOS unit adds or subtracts bandwidth on the basis of the amount of data it transmits *and* receives.
- DBA-None (2) specifies that the TAOS unit does not monitor traffic over the link.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-DBA-Monitor:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- The TAOS unit supports Ascend-DBA-Monitor only for MP+ calls.
- If both sides of the link have Ascend-DBA-Monitor set to DBA-None, Dynamic Bandwidth Allocation is disabled.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Dec-Channel-Count (237)

Description: Specifies the number of channels the TAOS unit removes when bandwidth changes during a call.

Usage: Specify a number from 1 to 32. The default value is 1.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Dec-Channel-Count:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- Ascend-Dec-Channel-Count does not apply if all channels of a link are nailed up (Ascend-Call-Type=Nailed).
- Ascend-Dec-Channel-Count applies only when the link is using MP+ encapsulation.
- You cannot clear a call by decrementing channels.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-History-Weigh-Type (239)" on page 4-87,

"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-DHCP-Maximum-Leases (134)

Description: Specifies the maximum number of dynamic addresses the TAOS unit can assign to Network Address Translation (NAT) for LAN clients that are using this connection.

Usage: Specify a value from 1 to 254. The default is 4.

Example: The following user profile specifies that the unit can assign a maximum of five dynamic addresses for the connection:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=11.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-DHCP-Maximum-Leases=5,
     Ascend-DHCP-Pool-Number=5,
     Ascend-DHCP-Reply=DHCP-Reply-Yes
```

See Also: "Ascend-DHCP-Pool-Number (148)" on page 4-55 and "Ascend-DHCP-Reply (147)" on page 4-56.

Ascend-DHCP-Pool-Number (148)

Description: Specifies the address pool from which the TAOS unit assigns a dynamic IP address to the Dynamic Host Configuration Protocol (DHCP) client.

Usage: Specify an integer from 1 to the number of address pools defined on the TAOS unit. The default value is 0 (zero), which specifies that the TAOS unit uses the first defined IP address pool.

Example: The following user profile specifies that the unit assigns a dynamic IP address from pool number 5:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=11.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-DHCP-Maximum-Leases=5,
     Ascend-DHCP-Pool-Number=5,
     Ascend-DHCP-Reply=DHCP-Reply-Yes
```

Dependencies: When the DHCP client requests an address, the TAOS unit allocates an IP address from one of its IP address pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment after the 30-minute period expires.

In its local memory, the TAOS unit keeps track of all the IP addresses it has assigned. Therefore, it loses the entries for current, unexpired IP address assignments when you reset it. If a client holds an unexpired IP address assignment when you reset the TAOS unit, the unit may assign the same address to a new client. These duplicate IP addresses cause network problems until the first assignment expires or one of the clients reboots.

See Also: "Ascend-DHCP-Maximum-Leases (134)" on page 4-55 and "Ascend-DHCP-Reply (147)" on page 4-56.

Ascend-DHCP-Reply (147)

Description: Specifies whether the TAOS unit processes Dynamic Host Configuration Protocol (DHCP) packets and acts as a DHCP server on this connection.

Usage: Specify one of the following settings:

- DHCP-Reply-No (0) specifies that the TAOS unit does not process DHCP packets, but routes or bridges DHCP packets as any other packet.
- DHCP-Reply-Yes (1) specifies that the TAOS unit processes DHCP packets. For a bridged connection, the TAOS unit responds to all DHCP requests. For a nonbridged connection, the TAOS unit responds only to Network Address Translation (NAT) for LAN DHCP packets.

Example: The following user profile specifies that the unit processes DHCP packets and acts as a DHCP server on the connection:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=11.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-DHCP-Maximum-Leases=5,
     Ascend-DHCP-Pool-Number=5,
     Ascend-DHCP-Reply=DHCP-Reply-Yes
```

See Also: "Ascend-DHCP-Maximum-Leases (134)" on page 4-55 and "Ascend-DHCP-Pool-Number (148)" on page 4-55.

Ascend-Dialout-Allowed (131)

Description: Specifies whether the user associated with an outgoing RADIUS user profile can use one of the TAOS unit's digital modems to dial out.

Usage: Specify one of the following settings:

- Dialout-Not-Allowed (0) specifies that the RADIUS user profile does not allow modem dialout. Dialout-Not Allowed is the default.
- Dialout-Allowed (1) specifies that the RADIUS user profile allows modem dialout.

Example: The following user profile specifies that the user Kevin can dial out using one of the TAOS unit's digital modems:

```
Kevin User-Password="kpassword"
   Service-Type=Framed-User,
```

```
   Framed-Protocol=MPP,
   Ascend-Dialout-Allowed=Dialout-Allowed
```

See Also: "Ascend-Dial-Number (227)" on page 4-57.

Ascend-Dial-Number (227)

Description: Specifies the phone number the TAOS unit dials to reach the router or node at the remote end of the link.

Usage: Specify a telephone number of up to 21 characters, limited to the following:

`1234567890()[]!z-*#|`

The TAOS unit sends only the numeric characters to place a call. The default value is null.

Example: The following profile specifies a dialout number of 555-1212:

```
joel-out User-Password="localpw", Service-Type=Outbound-User
   User-Name="joel",
   Framed-Protocol=PPP,
   Framed-IP-Address=10.2.3.31,
   Framed-IP-Netmask=255.255.255.0,
   Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
   Ascend-Dial-Number="555-1212",
   Ascend-Send-Auth=Send-Auth-PAP,
   Ascend-Send-Secret="remotepw"
```

See Also: "Ascend-Dialout-Allowed (131)" on page 4-56.

Ascend-Disconnect-Cause (195)

Description: Indicates the reason a connection went offline.

Usage: When a call disconnects, the TAOS unit typically sends the following message:

`call` *n* `CL OK u=` *username* `c=`*n* `p=`*m*

where:

- *n* specifies a disconnect code that indicates why the call disconnected.
- *m* specifies a progress code that indicates how far the call had progressed when it disconnected.

Table 4-11 provides a list of disconnect codes and their meanings.

Table 4-11. Disconnect codes

Disconnect code	Description
1	Should not be applied to any completed call, although the TAOS unit registers disconnect code 1 in accounting Checkpoint records. In any other case, if the TAOS unit displays disconnect code 1, contact Lucent Technical Support.

Table 4-11. Disconnect codes

Disconnect code	Description
2	Specifies an unknown disconnect, and is the default value that the TAOS unit displays for disconnects that have not been explicitly defined.
3	Call was disconnected.
4	CLID authentication failed.
5	RADIUS timeout occurred during authentication.
6	Successful authentication. The TAOS unit is configured to call the user back.
7	Pre-T310 disconnect timer was triggered.
9	No modem is available to accept the call.
10	Modem never detected Data Carrier Detect (DCD).
11	Modem detected DCD, but modem carrier was lost.
12	TAOS unit failed to successfully detect modem result codes.
13	TAOS unit failed to open a modem for an outgoing call.
14	TAOS unit failed to open a modem for an outgoing call while the modem diagnostic command was enabled.
15	TAOS unit failed to receive an OK from the modem.
16	Modem disconnected because of a stuck/full mailbox message queue of a modem chip.
17	Modem disconnected because of an inactive channel.
18	Timeout for graceful reboot forced a modem channel to disconnect.
20	User exited normally from the terminal server.
21	Terminal server timed out waiting for user input.
22	Forced disconnect occurred when the user was exiting a Telnet session.
23	No IP address was available when the client used a PPP or SLIP command.
24	Forced disconnect occurred when the user exited a raw TCP session.
25	Maximum login attempts exceeded.

Table 4-11. Disconnect codes

Disconnect code	Description
26	Attempted to start a raw TCP session, but raw TCP is disabled on the TAOS unit.
27	Control-C characters received during login.
28	Terminal-server session cleared ungracefully.
29	User closed a terminal-server virtual connection normally.
30	Terminal-server virtual connect cleared ungracefully.
31	Exit from Rlogin session.
32	Establishment of Rlogin session failed because of bad options.
33	TAOS unit lacks resources to process the terminal-server request.
35	MP+ session cleared because no null MP packets were received. A TAOS unit sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user was configured to send passwords by means of PAP, and the TAOS unit was configured to only accept passwords by means of CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	TAOS unit received a Terminate Request packet while LCP was in the open state.
46	TAOS unit received a Close Request from an upper layer, indicating graceful LCP closure.
47	TAOS unit cleared the call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	Disconnected MP session. The TAOS unit accepted an added channel, but cannot determine the call to which to add the new channel.
49	MP call was disconnected because no more channels could be added.
50	Telnet or raw TCP session tables are full.

Table 4-11. Disconnect codes

Disconnect code	Description
51	TAOS unit has exhausted Telnet or raw TCP resources.
52	For Telnet or raw TCP session, IP address is invalid.
53	For Telnet or raw TCP session, TAOS unit cannot resolve the host-name.
54	For Telnet or raw TCP session, TAOS unit received a bad or missing port number.
60	For Telnet or raw TCP session, host was reset.
61	For Telnet or raw TCP session, connection was refused.
62	For Telnet or raw TCP session, connection timed out.
63	For Telnet or raw TCP session, connection was closed by a foreign host.
64	For Telnet or raw TCP session, network was unreachable.
65	For Telnet or raw TCP session, host was unreachable.
66	For Telnet or raw TCP session, network admin was unreachable.
67	For Telnet or raw TCP session, host admin was unreachable.
68	For Telnet or raw TCP session, port was unreachable.
90	For Telnet or raw TCP session, no port is available.
100	Session timed out.
101	Invalid user.
102	Callback enabled.
103	TAOS unit disconnected the call because of a validation failure on an outgoing callback call.
105	Session timeout occurred because of encapsulation negotiations.
106	MP session timeout occurred.
115	Initiating call no longer active.
120	Requested protocol is disabled or unsupported.
150	Disconnect was requested by the RADIUS server.
151	Call was disconnected by the local administrator.

Table 4-11. Disconnect codes

Disconnect code	Description
152	Call was disconnected by means of SNMP.
160	TAOS unit disconnected a V.110 call because a timeout condition was triggered.
170	Timeout occurred while the unit was waiting to authenticate the remote device.
180	User was disconnected by executing Do Hangup from a VT100 interface.
171	TAOS unit disconnected the call when the PPP interface was released.
180	TAOS unit disconnected the call when the user entered the DO Hangup command.
181	Call cleared by the TAOS unit.
185	Signal lost from the remote end, typically because the remote modem was turned off.
190	Resource has been quiesced.
195	Maximum duration time was reached for the call.
201	TAOS unit has low memory.
210	TAOS unit's modem card stopped working while it had calls outstanding.
220	TAOS unit requires CBCP, but the client does not support it.
230	TAOS unit deleted the Vrouter.
240	TAOS unit disconnected the call on the basis of LQM measurements.
241	TAOS unit cleared a backup call.
250	IP Fax call cleared normally.
251	IP Fax call cleared because of low available memory.
252	TAOS unit detected an error for an incoming IP Fax call.
253	TAOS unit detected an error for an outgoing IP Fax call.
254	TAOS unit detected no available modem to support an IP Fax call.
255	TAOS unit detected a problem opening an IP Fax session.

Table 4-11. Disconnect codes

Disconnect code	Description
256	TAOS unit detected a problem when performing a TCP function during an IP Fax call.
257	IP Fax session cleared abnormally.
258	TAOS unit detected a problem when parsing the telephone number for an IP Fax call.
260	TAOS unit detected a problem when decoding IP Fax variables.
261	TAOS unit detected a problem when decoding IP Fax variables.
262	TAOS unit has no configured IP Fax server.
300	TAOS unit detected an X.25 error.
350	TAOS unit detected that an MP Master Card has failed.
370	TAOS unit disconnected the call because DNIS was denied.
400	TAOS unit disconnected the call because callback dialout failed.
420	TAOS unit disconnected the call because the unit could not find a private route table.
425	TAOS unit disconnected the call because the unit could not find a filter profile.
450	Bidirectional authentication failed.
801	An unallocated (unassigned) number was used.
802	No route exists to the specified transit network.
803	No route exists to the destination.
806	The channel was unacceptable.
816	Normal call clearing took place.
817	The user was busy.
818	The user is not responding.
819	There was no answer from the user (user alerted).
821	The call was rejected.
822	The number was changed.
827	The destination is out of order.

Table 4-11. Disconnect codes

Disconnect code	Description
828	An invalid number format (an incomplete address) was in use.
829	The facility was rejected.
830	The unit is responding to a Status Enquiry message.
831	An unspecified normal event occurred.
834	No circuit or channel is available.
838	The network is out of order.
841	A temporary failure occurred.
842	Switching equipment congestion occurred.
843	Access information was discarded.
844	The requested circuit or channel is not available.
845	The call was preempted.
847	A resource was unavailable.
850	The requested facility is not subscribed.
852	Outgoing calls are barred within the CUG.
854	Incoming calls are barred within the CUG.
858	The bearer capability is not presently available.
863	The service or option is not available.
865	The bearer capability is not implemented.
866	The channel type is not implemented.
869	The requested facility is not implemented.
881	An invalid call reference value was used.
882	The identified channel does not exist.
888	The unit specified an incompatible destination.
896	A mandatory information element is missing.
897	The message type does not exist or is not implemented.

Table 4-11. Disconnect codes

Disconnect code	Description
898	The message was not compatible with the call state, the message type does not exist, or the message type was not implemented.
899	The information element or parameter does not exist or is not implemented.
900	Invalid information element contents were detected.
901	The message is not compatible with the call state.
902	Recovery on timer expiration.
903	A parameter that does not exist or is not implemented was passed on.
911	A message with an unrecognized parameter was discarded.
927	An unspecified internetworking event has taken place.

Dependencies: The TAOS unit includes Ascend-Disconnect-Cause in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

See Also: "Ascend-Connect-Progress (196)" on page 4-42.

Ascend-Dsl-CIR-Recv-Limit (100)

Description: Specifies the maximum data rate (in kbps) to be received across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data rate limit were disabled, except that additional computations are performed unnecessarily.

Example: The following user profile specifies a maximum rate of 100 kbps for data received on the connection:

```
con7-1 User-Password="con7-1"
       Framed-Protocol=MPP,
       Framed-IP-Address=200.200.200.123,
       Framed-IP-Netmask=255.255.0.0,
       Ascend-Dsl-Rate-Type=Rate-Type-AdslCap,
       Ascend-Dsl-Rate-Mode=Rate-Mode-AutoBaud,
       Ascend-Dsl-Upstream-Limit=adslcap-up-1088000,
       Ascend-Dsl-Downstream-Limit=adslcap-dn-7168000,
       Ascend-Dsl-CIR-Recv-Limit=100,
       Ascend-Dsl-CIR-Xmit-Limit=101
```

Dependencies: The system activates configurable receive data-rate limits only for connections that use CAP-RADSL, SDSL, and unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

See Also: "Ascend-Dsl-CIR-Recv-Limit (100)" on page 4-64.

Ascend-Dsl-CIR-Xmit-Limit (101)

Description: Specifies the maximum data rate (in kbps) to be transmitted across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data rate limit were disabled, except that additional computations are performed unnecessarily.

Example: The following user profile specifies a maximum rate of 101 kbps for data transmitted on the connection:

```
con7-1 User-Password="con7-1"
       Framed-Protocol=MPP,
       Framed-IP-Address=200.200.200.123,
       Framed-IP-Netmask=255.255.0.0,
       Ascend-Dsl-Rate-Type=Rate-Type-AdslCap,
       Ascend-Dsl-Rate-Mode=Rate-Mode-AutoBaud,
       Ascend-Dsl-Upstream-Limit=adslcap-up-1088000,
       Ascend-Dsl-Downstream-Limit=adslcap-dn-7168000,
       Ascend-Dsl-CIR-Recv-Limit=100,
       Ascend-Dsl-CIR-Xmit-Limit=101
```

Dependencies: The system activates configurable transmit data-rate limits only for connections that use CAP-RADSL, SDSL, and unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

See Also: " Ascend-Dsl-CIR-Xmit-Limit (101)" on page 4-65.

Ascend-DSL-Downstream-Limit (99)

Description: Specifies the per-session ADSL-CAP, ADSL-DMT, or SDSL downstream data rate.

Usage: For an ADSL-CAP card, specify one of the following rates (in bps):

adslcap-dn-7168000 (0)
adslcap-dn-6272000 (1)
adslcap-dn-5120000 (2)
adslcap-dn-4480000 (3)
adslcap-dn-3200000 (4)
adslcap-dn-2688000 (5)
adslcap-dn-2560000 (6)
adslcap-dn-2240000 (7)
adslcap-dn-1920000 (8)

adslcap-dn-1600000 (9)
adslcap-dn-1280000 (10)
adslcap-dn-960000 (11)
adslcap-dn-640000 (12)

For an ADSL-DMT card, specify one of the following rates (in bps):

adsldmt-dn-auto (100)
adsldmt-dn-9504000 (101)
adsldmt-dn-8960000 (102)
adsldmt-dn-8000000 (103)
adsldmt-dn-7168000 (104)
adsldmt-dn-6272000 (105)
adsldmt-dn-5120000 (106)
adsldmt-dn-4480000 (107)
adsldmt-dn-3200000 (108)
adsldmt-dn-2688000 (109)
adsldmt-dn-2560000 (110)
adsldmt-dn-2240000 (111)
adsldmt-dn-1920000 (112)
adsldmt-dn-1600000 (113)
adsldmt-dn-1280000 (114)
adsldmt-dn-960000 (115)
adsldmt-dn-768000 (116)
adsldmt-dn-640000 (117)
adsldmt-dn-512000 (118)
adsldmt-dn-384000 (119)
adsldmt-dn-256000 (120)
adsldmt-dn-128000 (121)

For an SDSL card, specify one of the following rates (in bps):

sdsl-144000 (0)
sdsl-272000 (1)
sdsl-400000 (2)
sdsl-528000 (3)
sdsl-784000 (4)
sdsl-1168000 (5)
sdsl-1552000 (6)
sdsl-2320000 (7)

Example: The following profile specifies an SDSL downstream data rate of 144000 bps:

```
unit-1 User-Password="pw", Service-Type=Outbound-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.2.3.31
    Framed-IP-Netmask=255.255.255.0
    Ascend-Dsl-Rate-Type=Rate-Type-Sdsl
    Ascend-Dsl-Rate-Mode=Rate-Mode-AutoBaud,
```

```
    Ascend-DSL-Downstream-Limit=sdsl-144000,
    Ascend-DSL-Upstream-Limit=sdsl-144000
```

Dependencies: For SDSL connections, the value of Ascend-DSL-Downstream-Limit must match the value of Ascend-DSL-Upstream-Limit.

See Also: "Ascend-Dsl-Rate-Mode (97)" on page 4-67 and "Ascend-Dsl-Rate-Type (92)" on page 4-67.

Ascend-Dsl-Rate-Mode (97)

Description: Specifies the per-session DSL data-rate mode.

Usage: Specify one of the following settings:

- Rate-Mode-AutoBaud (1) specifies that a DSL modem should train up to a set data rate. If a DSL modem cannot train to this data rate, it connects to the closest rate to which it can train (the modem's ceiling rate).
- Rate-Mode-Single (2) specifies that a DSL modem should train to a single data rate, even if the DSL modem can possibly train at a higher or lower data rate. If the DSL modem cannot train to the specified single rate, the connection fails. Specify Rate-Mode-Single for an SDSL connection.

Example: The following profile specifies that the modem should train up to a set data rate:

```
unit-1 User-Password="pw", Service-Type=Outbound-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.2.3.31
    Framed-IP-Netmask=255.255.255.0
    Ascend-Dsl-Rate-Type=Rate-Type-Sdsl
    Ascend-Dsl-Rate-Mode=Rate-Mode-AutoBaud
```

See Also: "Ascend-DSL-Downstream-Limit (99)" on page 4-65 and "Ascend-Dsl-Rate-Type (92)" on page 4-67.

Ascend-Dsl-Rate-Type (92)

Description: Specifies the per-session modem type for rate control.

Usage: Specify one of the following settings:

- Rate-Type-Disabled (0) specifies that modem rate control is not active for this connection.
- Rate-Type-Sdsl (1) specifies that the per-session modem type is SDSL.
- Rate-Type-AdslCap (2) specifies that the per-session modem type is ADSL-CAP.
- Rate-Type-AdslDmtCell (3) specifies that the per-session modem type is Alcatel ADSL-DMT.
- Rate-Type-AdslDmt (4) specifies that the per-session modem type is ADSL-DMT.

Example: The following profile specifies SDSL as the per-session modem type:

```
unit-1 User-Password="pw", Service-Type=Outbound-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.2.3.31
    Framed-IP-Netmask=255.255.255.0
```

```
Ascend-Dsl-Rate-Type=Rate-Type-Sdsl
Ascend-Dsl-Rate-Mode=Rate-Mode-AutoBaud
```

See Also: "Ascend-DSL-Downstream-Limit (99)" on page 4-65 and "Ascend-Dsl-Rate-Mode (97)" on page 4-67.

Ascend-DSL-Upstream-Limit (98)

Description: Specifies the symmetrical data rate.

Usage: For an SDSL card, specify one of the following settings:

sdsl-144000 (0)
sdsl-272000 (1)
sdsl-400000 (2)
sdsl-528000 (3)
sdsl-784000 (4)
sdsl-1168000 (5)
sdsl-1552000 (6)
sdsl-2320000 (7)
sdsl-160000 (8)
sdsl-192000 (9)
sdsl-208000 (10)
sdsl-384000 (11)
sdsl-416000 (12)
sdsl-768000 (13)
sdsl-1040000 (14)
sdsl-1152000 (15)
sdsl-1536000 (16)
sdsl-1568000 (17)

For an ADSL-CAP card, specify one of the following values:

adslcap-up-1088000 (50)
adslcap-up-952000 (51)
adslcap-up-816000 (52)
adslcap-up-680000 (53)
adslcap-up-544000 (54)
adslcap-up-408000 (55)
adslcap-up-272000 (56)

For an ADSL-DMT card, specify one of the following values:

adsldmt-up-auto (150)
adsldmt-up-1088000 (151)
adsldmt-up-928000 (152)
adsldmt-up-896000 (153)
adsldmt-up-800000 (154)
adsldmt-up-768000 (155)
adsldmt-up-640000 (156)

adsldmt-up-512000 (157)

adsldmt-up-384000 (158)

adsldmt-up-256000 (159)

adsldmt-up-128000 (160)

Example: The following profile specifies an SDSL upstream data rate of 144000 bps:

```
unit-1 User-Password="pw", Service-Type=Outbound-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.2.3.31
    Framed-IP-Netmask=255.255.255.0
    Ascend-Dsl-Rate-Type=Rate-Type-Sdsl
    Ascend-Dsl-Rate-Mode=Rate-Mode-AutoBaud,
    Ascend-DSL-Downstream-Limit=sdsl-144000,
    Ascend-DSL-Upstream-Limit=sdsl-144000
```

Dependencies: For SDSL connections, the value of Ascend-DSL-Downstream-Limit must match the value of Ascend-DSL-Upstream-Limit.

See Also: "Ascend-DSL-Downstream-Limit (99)" on page 4-65.

Ascend-Egress-Enabled (58)

Description: Specifies whether the connection is an *Egress interface*—the exit point for all outgoing packets. The Egress feature provides a mechanism that controls the flow of bridged packets to a certain destination. In order to isolate customer premise PCs from one another other, packets arriving from each PC/CPE pair are sent to the configured Egress profile. Any interface can be designated as an Egress interface (Ethernet, ATM, Frame Relay, PPP, and so on).

Usage: Specify one of the following values:

- Egress-Enable-No (0) specifies that the interface is not the exit point for all outgoing bridged packets.
- Egress-Enabled-Yes (1) specifies that the interface is the exit point for all outgoing bridged packets.

Example: The following profile specifies an Egress interface:

```
permconn-test4-1 User-Password="ascend"
     Service-Type=Outbound-User,
     Framed-Protocol=FR,
     User-Name="p130-1-rad",
     Framed-Routing=None,
     Ascend-Route-IP=Route-IP-No,
     Ascend-Call-Type=Nailed,
     Ascend-Bridge=Bridge-Yes,
     Ascend-BIR-Bridge-Group=1,
     Ascend-FR-Profile-Name="fr1-rad",
     Ascend-Egress-Enabled=Egress-Enable-Yes
```

Dependencies: Bridged IP Routing (BIR) must be enabled for Ascend-Egress-Enabled to have any effect.

See Also: "Ascend-BIR-Bridge-Group (72)" on page 4-21, "Ascend-BIR-Enable (70)" on page 4-21, and "Ascend-BIR-Proxy (71)" on page 4-22.

Ascend-Endpoint-Disc (109)

Description: Specifies the LCP Endpoint Discriminator for the connection.

Usage: Specify the discriminator ID.

Example: The following example sets up an MP bundle using CLID and two-tier authentication with an Endpoint Discriminator:

```
510555-5555 User-Password="Ascend-CLID",
            Service-Type=Framed-User,
            Framed-Protocol=MPP,
            Ascend-Endpoint-Disc="123",
            Ascend-Require-Auth=Require-Auth

clara-p50 User-Password="ascend",
          Service-Type=Framed-User,
          Framed-Protocol=MPP,
          Ascend-Route-IP=Route-IP-Yes,
```

Dependencies: In order to use Ascend-Endpoint-Disc, you must configure Calling-Line ID (CLID) authentication, Dialed Number Information Service (DNIS) authentication, or two-stage authentication so that the profile is obtained before LCP negotiations are complete.

Ascend-Event-Type (150)

Description: Indicates one of the following:

- A cold-start notification, informing the accounting server that the TAOS unit has started up
- A session event, informing the authentication server that a session has begun

Usage: For a cold-start notification, Ascend-Event-Type=Ascend-Coldstart (1). For a session event, Ascend-Event-Type=Ascend-Session-Event (2).

Example: `Ascend-Event-Type=Ascend-Coldstart`

Dependencies: In a cold-start notification, the TAOS unit sends values for NAS-IP-Address, Ascend-Event-Type, and Ascend-Number-Sessions in an Ascend-Access-Event-Request packet (code 33). The RADIUS accounting server must send back an Ascend-Access-Event-Response packet (code 34) with the correct identifier to the TAOS unit.

In a session event, the TAOS unit sends values for User-Password, NAS-IP-Address, Ascend-Access-Event-Type, and Ascend-Number-Sessions in an Ascend-Access-Event-Request packet (code 33). The authentication server must send back an Ascend-Access-Event-Response packet (code 34) with the correct identifier to the TAOS unit.

See Also: "Ascend-Number-Sessions (202)" on page 4-110 and "NAS-IP-Address (4)" on page 4-156.

Ascend-Expect-Callback (149)

Description: Specifies whether a user dialing out should expect the remote end to call back.

Usage: Specify one of the following values:

- Expect-Callback-No (0) specifies that the caller does not wait for a callback after placing a call that does not connect. Expect-Callback-No is the default.
- Expect-Callback-Yes (1) specifies that the caller waits 90 seconds after placing a call that does not connect before attempting to place another call to the same number.

Example: The following dialout profile specifies that the user should expect the remote end to call back:

```
unit-1 User-Password="pw", Service-Type=Outbound-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.2.3.31
    Framed-IP-Netmask=255.255.255.0
    Ascend-Expect-Callback=Expect-Callback-Yes
```

See Also: "Ascend-Callback (246)" on page 4-26.

Ascend-FCP-Parameter (119)

Description: Specifies a user authorized to access resources behind a Secure Connect firewall. The Firewall Control Manager (FCM) uses the value of Ascend-FCP-Parameter to authenticate the user and retrieve access information.

Usage: Specify a user name.

Example: The following profile specifies four users authorized to access resources behind a Secure Connect firewall:

```
Jim User-Password="mypw"
      Service-Type=Login-User,
      Ascend-FCP-Parameter="agnt=137.175.85.10;comm=write|testkey",
      Ascend-FCP-Parameter="rmad=137.175.86.10",
      Ascend-FCP-Parameter="lcad=137.175.85.10",
      Ascend-FCP-Parameter="rule=all-2;time=30"
```

Dependencies: The Ascend-FCP-Parameter value is not sent directly to the TAOS unit. Rather, the value is sent to the FCM, which uses the information to build the SNMP messages that activate and deactivate rules in a Secure Connect firewall.

See Also: "Ascend-Remote-FW (110)" on page 4-124.

Ascend-Filter (91)

Description: Specifies a string-format filter, which can include an IP Type of Service (TOS) filter specification.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which you enter them is significant. If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile. A TOS filter value is specified in the following format:

```
iptos dir [dstip dest_ipaddr\subnet_mask]
[srcip src_ipaddr\subnet_mask][proto][destport cmp value]
[srcport cmp value][precedence value][type-of-service value]
```

Note: A filter definition cannot contain newlines. The syntax is shown here on multiple lines for printing purposes only.

Table 4-12 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-12.Ascend-Filter arguments

Keyword or argument	Description
`iptos`	Specifies an IP filter.
`dir`	Specifies filter direction. You can specify `in` (to filter packets coming into the TAOS unit) or `out` (to filter packets going out of the TAOS unit).
`dstip` *`dest_ipaddr \subnet_mask`*	If the `dstip` keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that destination address. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If the `dstip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets.
`srcip` *`src_ipaddr \subnet_mask`*	If the `srcip` keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that source address. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If the `srcip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets.
`proto`	A protocol number. A value of zero matches all protocols. If you specify a non-zero number, the TAOS unit compares it to the Protocol field in packets. For list of protocol numbers, see RFC 1700.
`dstport` *`cmp value`*	If the `dstport` keyword is followed by a comparison symbol and a port, the port is compared to the destination port of a packet. The comparison symbol can be `<` (less-than), `=` (equal), `>` (greater-than), or `!=` (not-equal). The port value can be one of the following names or numbers: `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), `talk` (517).

Table 4-12.Ascend-Filter arguments

Keyword or argument	Description
`srcport` *`cmp value`*	If the `srcport` keyword is followed by a comparison symbol and a port, the port is compared to the source port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or != (not-equal). The port value can be one of the following names or numbers: `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), `talk` (517).
`precedence` *`value`*	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. If a packet matches the filter, those bits are set to the specified value (most significant bit first): 000—Normal priority. 001—Priority level 1. 010—Priority level 2. 011—Priority level 3. 100—Priority level 4. 101—Priority level 5. 110—Priority level 6. 111—Priority level 7 (the highest priority).
`type-of-service` *`value`*	Type of Service (ToS) of the data stream. If a packet matches the filter, the system sets the four bits following the three most significant bits of the TOS byte to the specified value. Those four bits are used to choose a link based on the type of service. Specify one of the following values: Normal (0)—Normal service. Disabled (1)—Disables TOS. Cost (2)—Minimize monetary cost. Reliability (4)—Maximize reliability. Throughput (8)—Maximize throughput. Latency (16)—Minimize delay.

Example: The following RADIUS user profile defines a TOS filter for TCP packets (protocol 6) that are destined for a single host at 10.168.6.24. The packets must be sent on TCP port 23. For incoming packets that match this filter, the priority is set at level 2. This is a relatively low priority, which means that an upstream router that implements priority queuing may drop these packets when it becomes loaded. The commands also set TOS to prefer a low latency

connection. This means that the upstream router will choose a fast connection if one is available, even if it is higher cost, lower bandwidth, or less reliable than another available link.

```
John User-Password="jlhkjtn", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.168.6.120
    Framed-IP-Netmask=255.255.255.0
    Ascend-Filter="iptos in dstip 10.168.6.24/32
    dstport=23 precedence 010 type-of-service latency"
```

See Also: "Ascend-IP-TOS (88)" on page 4-94, "Ascend-IP-TOS-Apply-To (90)" on page 4-95, and "Ascend-IP-TOS-Precedence (89)" on page 4-96.

Ascend-Filter-Required (50)

Description: Specifies whether the TAOS unit establishes a call if the filter profile specified in the caller's RADIUS user profile cannot be found.

Usage: In a RADIUS user profile, specify one of the following values:

- Required-No (0) specifies that the TAOS unit establishes a call if the filter profile specified by the caller's RADIUS user profile cannot be found.
- Required-Yes (1) specifies that the TAOS unit does not establish a call if the filter profile specified by the caller's RADIUS user profile cannot be found.

Example: The following user profile specifies that the session disconnects the call if the Filter profile called `filter-c` is not found:

```
p50-v2 User-Password="my-password" Service-Type=Framed-User
    Framed-Protocol=PPP
    Framed-IP-Address=10.1.1.1
    Framed-IP-Netmask=255.0.0.0
    Filter-ID="filter-c"
    Ascend-Filter-Required=Required-Yes
```

Dependencies: If the call needs to be brought down, the cause code 425 results. If the call is allowed to come up, the system logs a notice-level message that the filter could not be found.

See Also: "Filter-ID (11)" on page 4-146.

Ascend-First-Dest (189)

Description: Records the destination IP address of the first packet the TAOS unit receives on a link after RADIUS authenticates the connection.

Usage: Ascend-First-Dest does not appear in a user profile and has no default value.

Example: `Ascend-First-Dest=10.1.2.3`

Dependencies: Ascend-First-Dest applies only if the session routes IP. The TAOS unit includes Ascend-First-Dest in an Accounting-Request packet when both of the following conditions are true:

- The session has been authenticated.

- The session has ended (Acct-Status-Type=Stop).

See Also: "Acct-Status-Type (40)" on page 4-5.

Ascend-Force-56 (248)

Description: Specifies whether the TAOS unit uses only the 56-Kbps portion of a channel, even when all 64 Kbps appear to be available:

Usage: Specify one of the following values:

- Force-56-No (0) specifies that the TAOS unit should use the entire 64 Kbps (when available). Force-56-No is the default.
- Force-56-Yes (1) specifies that the TAOS unit should use only the 56-Kbps portion of a channel.

Example: The following user profile specifies that the TAOS unit should use the entire 64 Kbps:

```
Michael User-Password="mypw", Service-Type=Framed-User
        Framed-Protocol=PPP,
        Framed-IP-Address=200.250.55.9,
        Framed-IP-Netmask=255.255.255.248,
        Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
        Framed-Compression=Van-Jacobson-TCP-IP,
        Ascend-Route-IP=Route-IP-Yes,
        Ascend-Force-56=Force-56-No,
        Ascend-Metric=2
```

Dependencies: Set Ascend-Force-56=Force-56-Yes when you place calls to European or Pacific Rim countries from within North America and the complete path cannot distinguish between the Switched-56 and Switched-64 data services.

Ascend-FR-08-Mode (10)

Description: Specifies whether Frame Relay traffic can be switched across a T3-ATM card without translating the data to Asynchronous Transfer Mode (ATM) format.

Usage: Specify one of the following settings:

- FR-08-Mode-No (0) specifies that the Frame Relay traffic is translated before it is switched.
- FR-08-Mode-Yes (1) enables FRF.8 Transparent mode support, specifying that the Frame Relay traffic is passed to the ATM switch without being translated.

Example: The following profile specifies the circuit between the Frame Relay and ATM interfaces, and enables FRF.8 Transparent mode support:

```
permconn-sys-1 User-Password="ascend",
   Service-Type=Outbound-User,
   User-Name="atm-endpoint",
   Framed-Protocol=ATM-FR-CIR,
   Ascend-Route-IP=Route-IP-No,
   Ascend-Group="111",
   Ascend-ATM-Vpi=100,
```

```
   Ascend-ATM-Vci=132,
   Ascend-FR-Circuit-Name="atmfr-1"
   Ascend-FR-08-Mode=FR-08-Mode-Yes
```

Dependencies: The setting FR-08-Mode-Yes applies only to a connection that uses Frame Relay circuit encapsulation.

See Also: "Ascend-FR-Circuit-Name (156)" on page 4-76.

Ascend-FR-Circuit-Name (156)

Description: Specifies the Permanent Virtual Connection (PVC) for which the user profile is an endpoint.

Usage: Specify a text string of up to 15 characters. The default value is null.

Example: In the following profile, the PVC is called `Circuit1`:

```
permconn-unit-1 User-Password="ascend", Service-Type=Outbound-User
   User-Name="EndPoint1",
   Ascend-FR-Profile-Name="FR Prof 1",
   Ascend-FR-DLCI=16,
   Ascend-FR-Circuit-Name="Circuit1",
   Framed-Protocol=FR-CIR
```

Dependencies: Consider the following:

- You can specify Ascend-FR-Circuit-Name only when Framed-Protocol=FR-CIR.
- The TAOS unit requires two profiles for a single PVC.
- The Frame Relay network switches matching pairs of Ascend-FR-Circuit-Name attributes to each other, so make sure that you specify the exact same name for Ascend-FR-Circuit-Name in each profile.

See Also: "Ascend-Ckt-Type (16)" on page 4-38.

Ascend-FR-DCE-N392 (162)

Description: Specifies the number of errors, during Ascend-FR-DCE-N393-monitored events, that causes the network side to declare the user side's procedures inactive.

Usage: Specify an integer from 1 to 10. The default value is 3.

Example: The following pseudo-user profile specifies that a total of nine errors causes the network side to declare the user side's procedures inactive:

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
```

```
Ascend-FR-DTE-N392=7,
Ascend-FR-DTE-N393=8,
Ascend-FR-DCE-N392=9,
Ascend-FR-DCE-N393=10
```

Dependencies: Consider the following:

- You should set Ascend-FR-DCE-N392 to a value less than Ascend-FR-DCE-N393.
- Ascend-FR-DCE-N392 does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-DCE-N393 (164)" on page 4-77 and "Ascend-FR-Type (159)" on page 4-84.

Ascend-FR-DCE-N393 (164)

Description: Specifies the DCE-monitored event count. The TAOS unit considers a link active if the event count does not reach the value of Ascend-FR-DCE-N393.

Usage: Specify a number from 1 to 10. The default value is 4.

Example: In the following profile, the DCE-monitored event count is 10:

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
      Ascend-FR-DTE-N392=7,
      Ascend-FR-DTE-N393=8,
      Ascend-FR-DCE-N392=9,
      Ascend-FR-DCE-N393=10
```

Dependencies: The Ascend-FR-DCE-N393 attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-Type (159)" on page 4-84.

Ascend-FR-Direct (219)

Description: Specifies whether the TAOS unit uses a Frame Relay Direct configuration for Frame Relay packets.

Usage: Specify one of the following values:

- FR-Direct-No (0) specifies that the TAOS unit does not use a Frame Relay Direct configuration. FR-Direct-No is the default.
- FR-Direct-Yes (1) specifies that the TAOS unit uses a Frame Relay Direct configuration.

Example: The following profile specifies a Frame Relay Direct connection:

```
permconn-unit-1 User-Password="ascend", Service-Type=Outbound-User
   User-Name="Michael",
   Ascend-FR-Direct=FR-Direct-Yes,
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-DLCI=72,
   Framed-Protocol=PPP
```

See Also: "Ascend-FR-Direct-DLCI (221)" on page 4-78 and "Ascend-FR-DLCI (179)" on page 4-79.

Ascend-FR-Direct-DLCI (221)

Description: Specifies the Data Link Connection Indicator (DLCI) for the user profile in a Frame Relay Direct configuration.

Usage: Specify an integer from 16 to 991. The default value is 16.

Example: The following profile specifies a Frame Relay Direct connection for DLCI 72:

```
permconn-unit-1 User-Password="ascend", Service-Type=Outbound-User
   User-Name="Michael",
   Ascend-FR-Direct=FR-Direct-Yes,
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-Direct-DLCI=72,
   Framed-Protocol=PPP
```

Dependencies: Ascend-FR-Direct-DLCI applies only if Ascend-FR-Direct=FR-Direct-Yes.

See Also: "Ascend-FR-Direct (219)" on page 4-77 and "Ascend-FR-Direct-Profile (220)" on page 4-78.

Ascend-FR-Direct-Profile (220)

Description: Specifies the name of the Frame Relay profile for a Frame Relay Direct configuration.

Usage: Specify the name of a Frame Relay profile. This profile connects to the Frame Relay switch handling the Data Link Connection Indicator (DLCI) specified by Ascend-FR-Direct-DLCI. You can specify up to 15 lowercase, alphanumeric characters. The default value is null.

Example: The following profile specifies a Frame Relay profile called `PacBell` for a Frame Relay Direct connection:

```
permconn-unit-1 User-Password="ascend", Service-Type=Outbound-User
   User-Name="Michael",
   Ascend-FR-Direct=FR-Direct-Yes,
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-Direct-DLCI=72,
   Framed-Protocol=PPP
```

Dependencies: Ascend-FR-Direct-Profile applies only if Ascend-FR-Direct=FR-Direct-Yes.

See Also: "Ascend-FR-Direct (219)" on page 4-77 and "Ascend-FR-Direct-DLCI (221)" on page 4-78.

Ascend-FR-DLCI (179)

Description: Specifies a Data Link Connection Indicator (DLCI) number for a Frame Relay gateway or switch. A DLCI is not an address, but a local label that identifies a logical link between a device and the Frame Relay switch. The switch uses the DLCI to route frames through the network, and the DLCI can change as frames are passed through multiple switches.

Usage: Specify an integer from 16 to 991. The default value is 16.

Example: The following profile specifies DLCI 57 for a Frame Relay gateway:

```
permconn-unit-2 User-Password="ascend", Service-Type=Outbound-User
   User-Name-"Catherine",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-Protocol=FR,
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n remote_router "
```

Dependencies: Ascend-FR-DLCI applies only if Ascend-FR-Direct=FR-Direct-No.

See Also: "Ascend-FR-Direct (219)" on page 4-77 and "Ascend-FR-Profile-Name (180)" on page 4-82.

Ascend-FR-DTE-N392 (163)

Description: Specifies the number of errors, during Ascend-FR-DTE-N393-monitored events, that causes the user side to declare the network side's procedures inactive.

Usage: Specify an integer from 1 to 10. The default value is 3.

Example: In the following profile, a total of seven errors causes the user side to declare the network side's procedures inactive:

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
      Ascend-FR-DTE-N392=7,
      Ascend-FR-DTE-N393=8,
      Ascend-FR-DCE-N392=9,
      Ascend-FR-DCE-N393=10
```

Dependencies: Consider the following:

- You should set Ascend-FR-DTE-N392 to a value less than Ascend-FR-DTE-N393.
- Ascend-FR-DTE-N392 does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: “Ascend-FR-DTE-N393 (165)” on page 4-80 and “Ascend-FR-Type (159)” on page 4-84.

Ascend-FR-DTE-N393 (165)

Description: Specifies the DTE-monitored event count. The TAOS unit considers a link active if the event count does not reach the value of Ascend-FR-DTE-N393.

Usage: Specify a number from 1 to 10. The default value is 4.

Example: In the following profile, the DTE-monitored event count is 8:

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
      Ascend-FR-DTE-N392=7,
      Ascend-FR-DTE-N393=8,
      Ascend-FR-DCE-N392=9,
      Ascend-FR-DCE-N393=10
```

Dependencies: The Ascend-FR-DTE-N393 attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: “Ascend-FR-Type (159)” on page 4-84.

Ascend-FR-Link-Mgt (160)

Description: Specifies the link management protocol the TAOS unit uses to communicate with the Frame Relay switch.

Usage: Specify one of the following values:

- Ascend-FR-No-Link-Mgt (0) specifies no link management, and is the default. The TAOS unit always considers a link active if no link management functions take place.
- Ascend-FR-T1-617D (1) specifies T1.617 Annex D link management.
- Ascend-FR-Q-933A (2) specifies Q.933 Annex A link management.

Example: To set up a Frame Relay profile called FR Prof 1 with a UNI-DCE interface and T1.617 Annex D link management, you would enter the following specifications:

```
frdlink-unit-1 User-Password="ascend", Service-Type=Outbound-User
     User-Name="FR Prof 1",
     Ascend-FR-Type=Ascend-FR-DCE,
     Ascend-FR-Nailed-Grp=1,
     Ascend-Data-Svc=Nailed-64K,
     Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

See Also: "Ascend-FR-Link-Status-DLCI (106)" on page 4-81.

Ascend-FR-Link-Status-DLCI (106)

Description: Specifies the DLCI to use for link management on the Frame Relay datalink.

Usage: Specify one of the following settings:

- Ascend-FR-LMI-Dlci-0 specifies DLCI 0 (zero).
- Ascend-FR-LMI-Dlci-1023 specifies DLCI 1023.

Example: The following profile specifies DLCI 1023:

```
frdlink-test-1 User-Password="ascend" Service-Type=Outbound-User
        Ascend-FR-Profile-Name="fr",
        Ascend-Call-Type=Nailed,
        Ascend-FR-Type=Ascend-FR-DTE,
        Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
        Ascend-FR-Nailed-Grp=1,
        Ascend-Data-Svc=Nailed-64K,
        Ascend-FR-Link-Status-Dlci=Ascend-FR-LMI-Dlci-1023,
        Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

See Also: "Ascend-FR-Link-Mgt (160)" on page 4-80.

Ascend-FR-N391 (161)

Description: Specifies the number of T391 polling cycles between full Status Enquiry messages.

Usage: Specify an integer from 1 to 255. The default value is 6, which indicates that after six status requests spaced Ascend-FR-T391 seconds apart, the UNI-DTE device requests a full status report.

Example: In the following example, the unit sends a Status Enquiry for Link Integrity Verification to Switch-3 every 10 seconds, and requests a Full status report every sixth enquiry (every 60 seconds):

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
      Ascend-FR-DTE-N392=7,
      Ascend-FR-DTE-N393=8,
      Ascend-FR-DCE-N392=9,
      Ascend-FR-DCE-N393=10
```

Dependencies: The Ascend-FR-N391 attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-T391 (166)" on page 4-83 and "Ascend-FR-Type (159)" on page 4-84.

Ascend-FR-Nailed-Grp (158)

Description: Associates a group of nailed-up channels with the Frame Relay profile.

Usage: Specify a number from 1 to 1024. The default value is 1.

Example: To set up a Frame Relay profile called FR Prof 1 that uses the nailed-up channels in group 5, you would enter the following specifications:

```
frdlink-unit-1 User-Password="ascend", Service-Type=Outbound-User
     User-Name="FR Prof 1",
     Ascend-FR-Type=Ascend-FR-DCE,
     Ascend-FR-Nailed-Grp=5,
     Ascend-Data-Svc=Nailed-64K,
     Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

Dependencies: Do not associate a group with more than one active Frame Relay profile.

See Also: "Ascend-Group (178)" on page 4-85.

Ascend-FR-Profile-Name (180)

Description: Specifies the name of the Frame Relay profile to use when the TAOS unit is configured as a Frame Relay gateway or Frame Relay switch.

Usage: Specify the name of a Frame Relay profile. This profile connects to the Frame Relay switch handling the Data Link Connection Indicator (DLCI) specified by Ascend-FR-DLCI. You can specify up to 15 lowercase, alphanumeric characters. The default value is null.

Example: The following profile specifies a Frame Relay profile called `PacBell`:

```
permconn-unit-2 User-Password="ascend", Service-Type=Outbound-User
   User-Name-"Catherine",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-Protocol=FR,
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n remote_router "
```

Dependencies: Ascend-FR-Profile-Name applies only if Ascend-FR-Direct=FR-Direct-No.

See Also: "Ascend-FR-DLCI (179)" on page 4-79.

Ascend-FR-SVC-Addr (12)

Description: Specifies a telephone number for the Frame Relay Switched Virtual Circuit (SVC). The link uses the telephone number as the Calling-Line ID (CLID) for outgoing calls.

Usage: Specify a telephone number.

Example: The following profile specifies that the SVC is enabled, and indicates its telephone number:

```
frdlink-test-1 User-Password="ascend"
   Service-Type=Outbound-User,
   Framed-Protocol=FR,
   Ascend-FR-Profile-Name="svca",
   Ascend-Call-Type=Nailed,
   Ascend-FR-Nailed-Grp=21,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
   Ascend-Data-Svc=Switched-64K,
   Ascend-SVC-Enabled=Ascend-SVC-Enabled-Yes,
   Ascend-FR-SVC-Addr="2225552222"
```

See Also: "Calling-Station-Id (31)" on page 4-145.

Ascend-FR-T391 (166)

Description: Specifies the Link Integrity Verification polling timer.

Usage: Specify a number of seconds from 5 to 30. The value should be less than that of Ascend-FR-T392. The default value is 10, which indicates that after Ascend-FR-N391 status requests spaced 10 seconds apart, the UNI-DTE device requests a full status report.

Example: In the following example, the unit sends a Status Enquiry for Link Integrity Verification to Switch-3 every 10 seconds, and requests a Full status report every sixth enquiry (every 60 seconds):

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
      Ascend-FR-DTE-N392=7,
      Ascend-FR-DTE-N393=8,
      Ascend-FR-DCE-N392=9,
      Ascend-FR-DCE-N393=10
```

Dependencies: The Ascend-FR-T391 attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-N391 (161)" on page 4-81, "Ascend-FR-T392 (167)" on page 4-83, and "Ascend-FR-Type (159)" on page 4-84.

Ascend-FR-T392 (167)

Description: Specifies the interval (in seconds) in which Status Enquiry messages should be received. The network records an error if it does not receive a Status Enquiry within the number of seconds you specify.

Usage: Specify a number of seconds from 5 to 30. The default value is 10.

Example: The following pseudo-user profile specifies that if the unit does not receive a Status Enquiry within a 15-second interval, the network records an error:

```
frdlink-sys-3 User-Password="ascend", Service-Type=Outbound-User
      Ascend-FR-Profile-Name="Switch-3",
      Ascend-Call-Type=Nailed,
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=52,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-N391=6,
      Ascend-FR-T391=10,
      Ascend-FR-T392=15,
      Ascend-FR-DTE-N392=7,
      Ascend-FR-DTE-N393=8,
      Ascend-FR-DCE-N392=9,
      Ascend-FR-DCE-N393=10
```

Dependencies: The Ascend-FR-T392 attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-Type (159)" on page 4-84.

Ascend-FR-Type (159)

Description: Specifies the kind of logical interface between the TAOS unit and the Frame Relay network on the datalink:

- The UNI (User to Network Interface) is the interface between an end-user and a network endpoint (a router or a switch) on the Frame Relay network.
- A DCE (Data Circuit-Terminating Equipment) is a device that connects the DTE (Data Terminal Equipment) to a communications channel, such as a telephone line.
- A DTE refers to a device that an operator uses, such as a computer or a terminal.
- NNI (Network-to-Network Interface) operation allows the TAOS unit to act as a Frame Relay switch communicating with another Frame Relay switch.

Usage: Specify one of the following values:

- Ascend-FR-DTE (0) specifies a UNI-DTE connection (the default). The TAOS unit operates as the user side, communicating with the network-side DCE switch.
- Ascend-FR-DCE (1) specifies a UNI-DCE connection. The TAOS unit operates as the network side, communicating with the user side (UNI-DTE) of a Frame Relay terminating unit.
- Ascend-FR-NNI (2) specifies an NNI connection. The TAOS unit performs both DTE and DCE link management.

Example: To set up a Frame Relay profile called FR Prof 1 with a UNI-DCE interface, you would enter the following specifications:

```
frdlink-unit-1 User-Password="ascend", Service-Type=Outbound-User
     User-Name="FR Prof 1",
     Ascend-FR-Type=Ascend-FR-DCE,
     Ascend-FR-Nailed-Grp=1,
```

```
Ascend-Data-Svc=Nailed-64K,
Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

See Also: "Ascend-FR-Link-Mgt (160)" on page 4-80.

Ascend-FT1-Caller (175)

Description: Specifies whether the TAOS unit initiates an FT1-B&O call, or waits for the remote end to initiate these types of calls.

Usage: Specify one of the following values:

- FT1-No (0) specifies that the TAOS unit waits for the remote end to initiate the call. FT1-No is the default.
- FT1-Yes (1) specifies that the TAOS unit initiates the call. If you choose this setting, the TAOS unit dials to bring online any switched circuits that are part of the call.

Example: The following pseudo-user profile specifies that the TAOS unit initiates the call:

```
permconn-Alameda-1 User-Password="ascend", Service-Type=Outbound-User
       User-Name="CA",
       Framed-Protocol=MPP,
       Framed-IP-Address=50.1.1.1,
       Framed-IP-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Call-Type=Nailed/Mpp,
       Ascend-Group="1,3,5,7",
       Ascend-FT1-Caller=FT1-Yes,
       Ascend-Target-Util=80,
       Ascend-History-Weigh-Type=History-Constant,
       Ascend-Seconds-Of-History=90,
       Ascend-Add-Seconds=30,
       Ascend-Remove-Seconds=30,
       Ascend-Maximum-Channels=10,
       Ascend-Inc-Channel-Count=2,
       Ascend-Dec-Channel-Count=2,
       Ascend-DBA-Monitor=DBA-Transmit-Recv
```

See Also: "Ascend-Call-Type (177)" on page 4-35.

Ascend-Group (178)

Description: Points to the nailed-up channels used by the profile's WAN link.

Usage: Your usage depends upon the value you specify for the Ascend-Call-Type attribute:

- If you set Ascend-Call-Type=Nailed, you can specify a number from 1 to 60 for Ascend-Group. The default value is 1.
- If you set Ascend-Call-Type=Nailed/Mpp, you can use the Ascend-Group attribute to assign multiple nailed-up groups to the profile. Specify a single number, or specify a list of numbers from 1 to 60, separated by commas, with no spaces. The default value is 1.

Example: For a Nailed/MPP connection to use the nailed-up channels in groups 1, 3, 5, and 7, you would configure a pseudo-user profile as follows:

```
permconn-Alameda-1 User-Password="ascend", Service-Type=Outbound-User
        User-Name="CA",
        Framed-Protocol=MPP,
        Framed-IP-Address=50.1.1.1,
        Framed-IP-Netmask=255.0.0.0,
        Ascend-Route-IP=Route-IP-Yes,
        Ascend-Metric=7,
        Framed-Routing=None,
        Ascend-Call-Type=Nailed/Mpp,
        Ascend-Group="1,3,5,7",
        Ascend-FT1-Caller=FT1-Yes,
        Ascend-Target-Util=80,
        Ascend-History-Weigh-Type=History-Constant,
        Ascend-Seconds-Of-History=90,
        Ascend-Add-Seconds=30,
        Ascend-Remove-Seconds=30,
        Ascend-Maximum-Channels=10,
        Ascend-Inc-Channel-Count=2,
        Ascend-Dec-Channel-Count=2,
        Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- Ascend-Group does not apply if the link consists entirely of switched channels.
- If you add channels for the Ascend-Group attribute, the TAOS unit adds the channels to any online connection that uses the group.
- Do not duplicate group numbers in active profiles.
- Although you can assign multiple groups to a user profile, do not mix the Serial WAN circuit with nailed-up T1/E1 channels.

See Also: "Ascend-FR-Nailed-Grp (158)" on page 4-82.

Ascend-Handle-IPX (222)

Description: Specifies how the TAOS unit handles NCP watchdog requests on behalf of IPX clients during IPX bridging.

Usage: Specify one of the following values:

- Handle-IPX-None (0) specifies that special IPX behavior does not take place. Choose this setting when the LAN on each side of the bridge has one or more IPX servers. Handle-IPX-None is the default.
- Handle-IPX-Client (1) specifies that the TAOS unit discards Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries. Choose Handle-IPX-Client when both these conditions are true:
  - The local LAN has IPX clients but no servers.
  - The TAOS unit is acting as a bridge to another LAN containing only IPX servers, or a combination of IPX servers and clients.

- Handle-IPX-Server (2) specifies that the TAOS unit discards all RIP and SAP periodic broadcasts and queries at its WAN interface. This mode enables the TAOS unit to bring down calls during idle periods without breaking client/server or peer-to-peer connections. Choose Handle-IPX-Server when both these conditions are true:
  - The TAOS unit is acting as a bridge to a remote LAN with IPX clients, but no servers.
  - The local LAN contains only IPX servers, or a combination of IPX clients and servers.

Example: The following user profile specifies an IPX bridging link in which the local Ethernet supports NetWare clients, and the remote network supports both NetWare servers and clients:

```
unit1 User-Password="m2dan", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Ascend-Route-IPX=Route-IPX-No,
      Ascend-Bridge=Bridge-Yes,
      Ascend-Handle-IPX=Handle-IPX-Client,
      Ascend-Netware-timeout=30
```

Dependencies: Consider the following:

- If you specify Ascend-Handle-IPX=Handle-IPX-Server, you must also specify a value for the Ascend-Netware-timeout attribute, indicating the maximum length of idle time during which the TAOS unit performs watchdog spoofing for NetWare connections.
- If the connection does not bridge (Ascend-Bridge=Bridge-No), the Ascend-Handle-IPX attribute does not apply.
- If the TAOS unit on one LAN sets Ascend-Handle-IPX=Handle-IPX-Server, and the LAN on the other side of the connection has only NetWare clients, the TAOS unit on the client-only LAN should set Ascend-Handle IPX=Handle-IPX-Client. If both LANs contain servers, both sides of the connection should set Ascend-Handle-IPX=Handle-IPX-None.
- Although Ascend-Handle-IPX does not apply if Ascend-Bridge=Bridge-No, the TAOS unit automatically performs watchdog spoofing just as though you had set Ascend-Handle-IPX=Handle-IPX-Server. However, the TAOS unit does not filter as though you had set Ascend-Handle-IPX=Handle-IPX-Server.

See Also: “Ascend-Bridge (230)” on page 4-22 and “Ascend-Netware-timeout (223)” on page 4-108.

Ascend-History-Weigh-Type (239)

Description: Specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data.

Usage: Specify one of the following settings:

- History-Constant (0) gives equal weight to all samples taken during the historical time period specified by the Ascend-Seconds-Of-History attribute. When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as more recent samples.

- History-Linear (1) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History. The weighting grows at a linear rate.
- History-Quadratic (2) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Ascend-Seconds-Of-History attribute. The weighting grows at a quadratic rate. History-Quadratic is the default.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-History-Weigh-Type:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Home-Agent-IP-Addr (183)

Description: Indicates the IP address of the Home Agent used for the Mobile Client.

Usage: The Ascend-Home-Agent-IP-Addr attribute appears in an accounting Stop record under the following conditions:

- The session has ended.
- The Accounting-Request packet includes Acct-Status-Type=Stop.
- The session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).

Example: `Ascend-Home-Agent-IP-Addr=10.1.2.3`

See Also: "Ascend-Home-Agent-UDP-Port (186)" on page 4-89 and "Ascend-Home-Network-Name (185)" on page 4-89.

Ascend-Home-Agent-UDP-Port (186)

Description: Specifies the UDP port number to which the Foreign Agent directs Ascend Tunnel Management Protocol (ATMP) messages.

Usage: Specify a UDP port number from 0 to 65535. The default value is 5150.

Example: In the following example, the Foreign Agent dials the connection to the primary Home Agent and requests a tunnel on port 8877. If that attempt fails, it dials the connection to the secondary Home Agent and requests a tunnel on port 4000.

```
user1 User-Password="pass1"
   Service-Type=Framed-User,
   Framed-IP-Address=10.1.1.1,
   Framed-IP-Netmask=255.255.255.255,
   Tunnel-Type=ATMP,
   Tunnel-Server-Endpoint="2.2.2.2:8877",
   Ascend-Secondary-Home-Agent="3.3.3.3",
   Ascend-Home-Agent-UDP-Port=4000
```

Dependencies: If you specify a value for the *udp_port* argument of Ascend-Server-Endpoint or Ascend-Secondary-Home-Agent, or if you accept the default of 5150 for *udp_port*, you need not specify the Ascend-Home-Agent-UDP-Port attribute.

See Also: "Ascend-Secondary-Home-Agent (130)" on page 4-128 and "Tunnel-Server-Endpoint (67)" on page 4-165.

Ascend-Home-Network-Name (185)

Description: Specifies the name of the Connection profile that defines the link on which the Home Agent sends all packets it receives from the Mobile Client during Ascend Tunnel Management Protocol (ATMP) operation.

Usage: Specify the name of the Home Agent's Connection profile. The default value is null.

Example: In the following example, the Home Agent uses the Homenet Connection profile to the Home Network:

```
Node1 User-Password="Top-secret"
      Framed-Protocol=PPP,
      Ascend-Route-IP=Route-IP-Yes,
      Framed-IP-Address=200.1.1.2,
      Framed-IP-Netmask=255.255.255.0,
      Tunnel-Type=ATMP,
      Tunnel-Password="mypw",
      Tunnel-Server-Endpoint=10.8.9.10,
      Ascend-Home-Network-Name="Homenet"
```

Dependencies: You must specify a value for the Ascend-Home-Network-Name attribute only if the Home Agent is a gateway.

See Also: "Tunnel-Password (69)" on page 4-162, "Tunnel-Server-Endpoint (67)" on page 4-165, and "Tunnel-Type (64)" on page 4-166.

Ascend-Host-Info (252)

Description: Specifies a list of hosts to which a user can establish a Telnet session.

Usage: You can specify up to 10 Ascend-Host-Info entries in a user profile. Enter your setting in the following format:

```
Ascend-Host-Info="IP_address text"
```

where *IP_address* specifies the IP address of each host, and *text* describes each host. You can enter up to 31 characters for *text*. The RADIUS server assigns each entry a number. When the user selects the number, the terminal server initiates a Telnet session with the host at the specified IP address.

Example: To set up a host list for a TAOS unit named Cal, you would configure a pseudo-user profile as follows:

```
banner-Cal User-Password="ascend", Service-Type=Outbound-User
     Reply-Message="Up to 16 lines of up to 80 characters each",
     Reply-Message="will be accepted. ",
     Reply-Message="Additional lines will be ignored.",
     Reply-Message="",
     Ascend-Host-Info="1.2.3.4 Berkeley",
     Ascend-Host-Info="1.2.3.5 Alameda",
     Ascend-Host-Info="1.2.36 San Francisco"
```

See Also: "Reply-Message (18)" on page 4-159.

Ascend-IF-Netmask (153)

Description: Specifies the subnet mask in use for the local numbered interface.

Usage: Specify a subnet mask consisting of four numbers from 0 to 255, separated by periods. The default value is 0.0.0.0.

Example: The following RADIUS user profile specifies a subnet mask of 255.255.255.255 for the local numbered interface:

```
numbered User-Password="localpw"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-IP-Address=10.9.1.213,
   Framed-IP-Netmask=255.255.255.252,
   Ascend-PPP-Address=10.9.1.212,
   Ascend-IF-Netmask=255.255.255.252
```

See Also: "Ascend-PPP-Address (253)" on page 4-112 and "Ascend-Remote-Addr (154)" on page 4-123.

Ascend-Inc-Channel-Count (236)

Description: Specifies the number of channels the TAOS unit adds when bandwidth changes during a call.

Usage: Specify a number from 1 to 32. The default value is 1.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Inc-Channel-Count:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- Ascend-Inc-Channel-Count does not apply if all channels of a link are nailed up (Ascend-Call-Type=Nailed).
- Ascend-Inc-Channel-Count applies only if the link is using MP+ encapsulation.
- MP+ calls cannot exceed 32 channels.
- The sum of Ascend-Base-Channel-Count and Ascend-Inc-Channel-Count must not exceed the maximum number of channels available.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-IP-Direct (209)

Description: Specifies the IP address to which the TAOS unit redirects packets from the user. When you include this attribute in a user profile, the TAOS unit bypasses all internal routing tables and simply sends all packets it receives on the connection's WAN interface to the specified IP address. Ascend-IP-Direct only affects packets *from* the user. It does not affect

packets that go *to* the user. The TAOS unit uses its internal routing scheme to route packets to the user.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. If you accept the default, the TAOS unit does not redirect IP traffic.

Example: To specify that the TAOS unit redirects incoming packets to the host at IP address 10.2.3.11, you could configure a user profile as follows:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=10.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None
```

Dependencies: Consider the following:

- You can specify the Ascend-IP-Direct attribute only if IP routing is in use and Framed-Protocol is not set to FR.
- Do not set Ascend-IP-Direct and Ascend-FR-Direct in the same user profile. If you do, an error occurs.
- Ascend-IP-Direct connections typically turn off RIP. If you configure the connection to receive RIP, the TAOS unit forwards all RIP packets it receives to the IP address you specify. To turn off RIP, set Framed-Routing=None.

See Also: "Framed-Routing (10)" on page 4-152.

Ascend-IP-Pool-Chaining (85)

Description: Specifies whether IP pool chaining is enabled.

Usage: Specify one of the following values:

- IP-Pool-Chaining-No (0) disables IP pool chaining.
- IP-Pool-Chaining-Yes (1) enables IP pool chaining. When IP pool chaining is enabled, contiguous pools are treated as one *pool space* with shared addresses. When the system assigns an address to a user, it begins searching for an available address in the first pool of the chain and stops when it finds an available address or encounters a null pool definition. The pools within a chain must be defined in a contiguous sequence.

Example: The following profile contains two IP pool chains (for pools 1, 2, 3, and pools 7, 8, 9), with each pool chain containing 30 addresses:

```
pools-JFAN-TAOS User-Password="ascend", Service-Type=Outbound-User
    Ascend-IP-Pool-Chaining=IP-Pool-Chaining-Yes,
    Ascend-IP-Pool-Definition="1 11.168.6.10 10",
    Ascend-IP-Pool-Definition="2 12.168.6.10 10",
    Ascend-IP-Pool-Definition="3 13.168.6.10 10",
    Ascend-IP-Pool-Definition="7 17.168.6.10 10",
    Ascend-IP-Pool-Definition="8 18.168.6.10 10",
    Ascend-IP-Pool-Definition="9 19.168.6.10 10"
```

Dependencies: Consider the following:

- Address pools must be defined, either locally or in a RADIUS pseudo-user profile.
- Address assignment and VSA-compatibility mode must be enabled locally.
- The value of Ascend-IP-Pool-Chaining overrides any pool-chaining setting specified locally.

See Also: "Ascend-Assign-IP-Pool (218)" on page 4-10 and "Ascend-IP-Pool-Definition (217)" on page 4-93.

Ascend-IP-Pool-Definition (217)

Description: Specifies the first address in an IP address pool, as well as the number of addresses in the pool.

Usage: The Ascend-IP-Pool-Definition attribute has the following format:

`Ascend-IP-Pool-Definition="`*`num first_ipaddr max_entries`* `[`*`vrouter_name`*`]"`

Table 4-13 describes each Ascend-IP-Pool-Definition argument.

Table 4-13. Ascend-IP-Pool-Definition arguments

Argument	Specifies
num	Number of the pool. The default value is 1. Specify pool numbers starting with 1, unless you have defined pools using the TAOS unit's configuration interface, and do not wish to override those settings. In that case, for the *num* argument, start with one plus the highest number you used for an IP address pool on the TAOS unit. For example, if you set up address pools 1 through 5 on the TAOS unit, specify pool numbers starting with 6 in RADIUS.
first_ipaddr	First IP address in the address pool. The address you specify should not accept a subnet mask, because it always becomes a host route. The default value is 0.0.0.0. **Note:** In Windows, the default subnet mask for PPP interfaces is 255.255.255.0. Therefore, if NetBIOS over IP is enabled, connected Windows users will broadcast to .255, causing a performance problem for anyone connected at that address.
max_entries	Maximum number of IP addresses in the pool. The TAOS unit assigns addresses sequentially, from *first_ipaddr* on, up to the limit of addresses specified by *max_entries*. The default value is 0 (zero). You can specify up to 500 addresses.
vrouter_name	Name of the Virtual Router (VRouter) to which the IP address pool belongs.

Example: In the following example, an administrator configures a pseudo-user profile to create two address pools. Address pool #1 contains a block of 7 IP addresses from 10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48.

```
pools-Alameda User-Password="ascend", Service-Type=Outbound-User
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
```

See Also: "Ascend-Assign-IP-Pool (218)" on page 4-10.

Ascend-IPSEC-Profile (73)

Description: Specifies an IPSEC profile that describes the IPsec transforms and endpoints to use for the connection.

Usage: Enter a text string.

Example: Following are sample RADIUS profiles that reference the IPSEC profile called `securegw-1`:

```
tcpapp1 User-Password="secret-1"
    Service-Type=Login-User,
    Login-Service=TCP-Clear,
    Login-IP-Host=10.10.10.1,
    Login-TCP-Port=23,
    Login-IP-Host=10.10.10.2,
    Login-TCP-Port=125,
    Ascend-IPSEC-Profile=securegw-1
tcpapp2 User-Password="secret-2"
    Service-Type=Login-User,
    Login-Service=TCP-Clear,
    Login-IP-Host=10.10.10.1,
    Login-TCP-Port=23,
    Login-IP-Host=10.10.10.2,
    Login-TCP-Port=125,
    Ascend-IPSEC-Profile=securegw-1
tcpapp3 User-Password="secret-3"
    Service-Type=Login-User,
    Login-Service=TCP-Clear,
    Login-IP-Host=10.10.10.1,
    Login-TCP-Port=23,
    Login-IP-Host=10.10.10.2,
    Login-TCP-Port=125,
    Ascend-IPSEC-Profile=securegw-1
```

See Also: "Service-Type (6)" on page 4-159.

Ascend-IP-TOS (88)

Description: Specifies the Type-of-Service (TOS) of the data stream.

Usage: The value you specify sets the four bits following the three most significant bits of the TOS byte. Specify one of the following values:

- IP-TOS-Normal (0) specifies normal service.
- IP-TOS-Disabled (1) disables TOS.
- IP-TOS-Cost (2) minimizes monetary cost.
- IP-TOS-Reliability (4) maximizes reliability.
- IP-TOS-Throughput (8) maximizes throughput.
- IP-TOS-Latency (16) minimizes delay.

Example: The following RADIUS user profile specifies maximum throughput. The upstream router will choose a high-bandwidth connection is one is available, even if the link is less reliable, or has a higher cost or higher latency than another available link:

```
jfan-pc User-Password="johnfan", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.168.6.120
    Framed-IP-Netmask=255.255.255.0
    Framed-Routing=3
    Ascend-IP-TOS=IP-TOS-Throughput
    Ascend-IP-TOS-Precedence=IP-TOS-Precedence-Pri-Six
    Ascend-IP-TOS-Apply-To=IP-TOS-Apply-To-Incoming
```

See Also: “Ascend-IP-TOS-Apply-To (90)” on page 4-95 and “Ascend-IP-TOS-Precedence (89)” on page 4-96.

Ascend-IP-TOS-Apply-To (90)

Description: Specifies the direction in which Type-of-Service (TOS) is enabled.

Usage: Specify one of the following values:

- IP-TOS-Apply-To-Incoming (1024) specifies that bits are set in packets received on the interface. This setting is the default.
- IP-TOS-Apply-To-Outgoing (2048) specifies that bits are set in outbound packets only.
- IP-TOS-Apply-To-Both (3072) specifies that both incoming and outgoing packets are tagged.

Example: The following RADIUS user profile specifies that bits are set in received packets only:

```
jfan-pc User-Password="johnfan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=10.168.6.120
     Framed-IP-Netmask=255.255.255.0
     Framed-Routing=3
     Ascend-IP-TOS=IP-TOS-Throughput
     Ascend-IP-TOS-Precedence=IP-TOS-Precedence-Pri-Six
     Ascend-IP-TOS-Apply-To=IP-TOS-Apply-To-Incoming
```

See Also: “Ascend-IP-TOS (88)” on page 4-94 and “Ascend-IP-TOS-Precedence (89)” on page 4-96.

Ascend-IP-TOS-Precedence (89)

Description: Specifies the priority level of the data stream.

Usage: The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled, those bits can be set to one of the following values (most significant bit first):

- IP-TOS-Precedence-Pri-Normal (0) specifies normal priority.
- IP-TOS-Precedence-Pri-One (32) specifies priority level 1.
- IP-TOS-Precedence-Pri-Two (64) specifies priority level 2.
- IP-TOS-Precedence-Pri-Three (96) specifies priority level 3.
- IP-TOS-Precedence-Pri-Four (128) specifies priority level 4.
- IP-TOS-Precedence-Pri-Five (160) specifies priority level 5.
- IP-TOS-Precedence-Pri-Six (192) specifies priority level 6.
- IP-TOS-Precedence-Pri-Seven (224) specifies priority level 7 (the highest priority).

Example: The following RADIUS user profile sets the priority of the packets in the data stream at 6. An upstream router that implements priority queuing will not drop the packets until it has dropped all packets of a lower priority.

```
jfan-pc User-Password="johnfan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=10.168.6.120
     Framed-IP-Netmask=255.255.255.0
     Framed-Routing=3
     Ascend-IP-TOS=IP-TOS-Throughput
     Ascend-IP-TOS-Precedence=IP-TOS-Precedence-Pri-Six
     Ascend-IP-TOS-Apply-To=IP-TOS-Apply-To-Incoming
```

See Also: "Ascend-IP-TOS (88)" on page 4-94 and "Ascend-IP-TOS-Apply-To (90)" on page 4-95

Ascend-IPX-Alias (224)

Description: Specifies an IPX network number to use when connecting to IPX routers that require numbered interfaces.

Usage: Specify an IPX network number. The default value is 0 (zero). RADIUS requires that the Ascend-IPX-Alias attribute have a decimal value (base 10), but IPX network numbers generally have hexadecimal values (base 16). In order to give the Ascend-IPX-Alias attribute a value, you must convert the hexadecimal IPX network number to a decimal value for use in the user profile.

Example: The following profile specifies the IPX network number as the decimal value 3724805632, which corresponds to the hexadecimal value DE040600:

```
ipx-unit User-Password="ascend", Service-Type=Outbound-User
         User-Name="cs",
         Ascend-Dial-Number="96135494",
         Framed-Protocol=PPP,
         Ascend-Route-IP=Route-IP-Yes,
         Framed-IP-Address=10.10.10.11,
```

```
        Framed-IP-Netmask=255.255.255.255,
        Framed-Routing=None,
        Ascend-Bridge=Bridge-No,
        Ascend-Route-IPX=Route-IPX-Yes,
        Ascend-IPX-Peer-Mode=IPX-Peer-Router,
        Framed-IPX-Network=109255736,
        Ascend-IPX-Alias=3724805632,
        Ascend-Netware-timeout=10,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-Link-Compression=Link-Comp-None,
        Ascend-Metric=2
```

See Also: "Ascend-IPX-Peer-Mode (216)" on page 4-98, "Ascend-IPX-Route (174)" on page 4-98, and "Ascend-Route-IPX (229)" on page 4-127.

Ascend-IPX-Header-Compression (65)

Description: Specifies whether the connection uses IPX header compression.

Usage: Specify one of the following values:

- Ascend-IPX-Header-Compression-No (0) disables IPX header compression for the connection.
- Ascend-IPX-Header-Compression-Yes (1) enables IPX header compression for the connection.

Example: The following user profile specifies a connection to a Novell LAN, and indicates that the link uses IPX header compression:

```
sitebw User-Password="mypw"
    Service-Type=Framed-User,
    Framed-Protocol=MPP,
    Ascend-Route-IPX=Route-IPX-Yes,
    Ascend-IPX-Peer-Mode=IPX-Peer-Router,
    Ascend-IPX-Header-Compression=Ascend-IPX-Header-Compression-Yes
```

See Also: "Ascend-Link-Compression (233)" on page 4-99, "Ascend-PPP-VJ-Slot-Comp (210)" on page 4-114, and "Framed-Compression (13)" on page 4-146.

Ascend-IPX-Node-Addr (182)

Description: Specifies a unique IPX node address on the network specified by Framed-IPX-Network. This value completes the IPX address of a Mobile Client.

Usage: Specify a 12-digit ASCII string enclosed in double-quotes. The RADIUS server passes the attributes in the Mobile Client's profile to the Foreign Agent. The Foreign Agent sends these attributes when connecting with the Home Agent.

Example: The following user profile specifies an IPX node address for a Mobile Client in Gateway mode:

```
mobile-ipx User-Password="unit"
       Service-Type=Framed-User,
```

```
Ascend-Route-IPX=Route-IPX-Yes,
Framed-Protocol=PPP,
Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
Ascend-Route-IPX=Route-IPX-Yes,
Framed-IPX-Network=40000000,
Ascend-IPX-Node-Addr=12345678,
Ascend-Home-Agent-IP-Addr =200.168.6.18,
Ascend-Home-Network-Name="Dave's TAOS unit",
Ascend-Home-Agent-Password="mypw"
```

See Also: "Framed-MTU (12)" on page 4-149.

Ascend-IPX-Peer-Mode (216)

Description: Specifies whether the caller associated with the user profile is an Ethernet client with its own IPX network address, or a dial-in PPP client.

Dial-in clients do not belong to an IPX network, so you must assign them an IPX network number. When you do so, a dial-in client can establish a routing connection with the TAOS unit. You must use the TAOS configuration interface to define a virtual IPX network. The TAOS unit advertises the route to the virtual network, and assigns it as the network address for dial-in clients.

Usage: Specify one of the following values:

- IPX-Peer-Router (0) specifies that the caller is on the Ethernet network and has its own IPX address. IPX-Peer-Router is the default.
- IPX-Peer-Dialin (1) specifies that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface. This setting causes the TAOS unit to assign the caller an IPX address derived from the value of IPX-Dialin-Pool.

Example: The following user profile specifies that the caller is on the Ethernet interface:

```
sitebw User-Password="mypw"
    Service-Type=Framed-User,
    Framed-Protocol=MPP,
    Ascend-Route-IPX=Route-IPX-Yes,
    Ascend-IPX-Peer-Mode=IPX-Peer-Router
```

Dependencies: If the client does not supply its own unique node number, the TAOS unit assigns a unique node number to the client as well. The TAOS unit does not send IPX RIP and SAP advertisements across the connection and ignores IPX RIP and SAP advertisements it receives from the remote end. However, it does respond to IPX RIP and SAP queries it receives from dial-in clients.

See Also: "Ascend-IPX-Route (174)" on page 4-98 and "Ascend-Route-IPX (229)" on page 4-127.

Ascend-IPX-Route (174)

Description: Enables you to configure a static IPX route in a pseudo-user profile.

Usage: To configure a static IPX route, use the following format:

```
Ascend-IPX-Route="profile_name network# [node#] [socket#]
[server_type] [hop_count] [tick_count] [server_name]"
```

Table 4-14 describes each Ascend-IPX-Route argument.

Table 4-14. Ascend-IPX-Route arguments

Argument	Specifies
profile_name	RADIUS user profile the TAOS unit uses to reach the network. The default value is null.
network#	Unique internal network number for the NetWare server. The default value is 00000000.
node#	Node number for the NetWare server. The default value is 0000000000001 (the typical node number for a NetWare file server.)
socket#	Socket number for the NetWare server. Typically, NetWare file servers use socket 0451. The default value is 0000. The number you specify must be a well-known socket number. Services that use dynamic socket numbers might use a different socket each time they load. To bring up a connection to a remote service that uses a dynamic socket number, specify a master server that uses a well-known socket number.
server_type	SAP service type of the NetWare server. NetWare file servers have SAP service type 0004. The default value is 0000.
hop_count	Distance to the destination network, in hops. The default value is 1.
tick_count	Distance to the destination network, in IBM PC clock ticks (one-eighteenth of a second). This value is for round-trip timer calculation and for determining the nearest server of a given type. The default value is 12.
server_name	Name of an IPX server. The default value is null.

Example: To define an IPX route, you would configure a pseudo-user profile as follows:

```
ipxroute-CA-1 User-Password="ascend", Service-Type=Outbound-User
        Ascend-IPX-Route="def 6 7 8 9 10"
```

See Also: "Ascend-IPX-Alias (224)" on page 4-96,
"Ascend-IPX-Peer-Mode (216)" on page 4-98, and
"Ascend-Route-IPX (229)" on page 4-127.

Ascend-Link-Compression (233)

Description: Specifies the link-compression method to use for PPP-encapsulated packets transmitted and received on the connection.

Usage: You can specify one of the following values:

- Link-Comp-None (0) disables data compression. Link-Comp-None in the default.
- Link-Comp-Stac (1) enables a modified version of draft 0 of the Compression Control Protocol (CCP), which predates RFC 1974. Older equipment supports this compression method.
- Link-Comp-Stac-Draft-9 (2) enables the compression/decompression algorithm specified in draft 9 of the Stac LZS compression protocol, which is described in RFC 1974. Most devices use this compression method.
- Link-Comp-MS-Stac (3) enables the compression/decompression algorithm used by Windows 95 clients.

Example: Following is a sample RADIUS user profile that uses Stac-9 compression:

```
user-1 User-Password="localpw"
    Service-Type=Framed-User,
    Framed-Protocol=PPP,
    Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
    Framed-IP-Address=10.1.1.1,
    Framed-IP-Netmask=255.255.255.0
```

Dependencies: During the negotiation phase of the connection, both sides must agree to use the specified method.

By default, NetWare relies on the Data Link layer (also called Layer 2) to validate and guarantee data integrity. When you configure Stac compression, the system performs an eight-bit checksum, which is inadequate for NetWare data. Therefore, for NetWare connections, carry out one of the following tasks:

- Specify Link-Comp-Stac-Draft-9 or Link-Comp-MS-Stac, which use a more robust error-checking method.
- Disable link compression by setting Ascend-Link-Compression=Link-Comp-None. When you do so, the TAOS unit guarantees data integrity by means of PPP.
- Accept the default Link-Comp-Stac setting, and enable IPX checksums on your NetWare servers and clients. Both the server and the client must support IPX checksums. If you enable checksums on your servers, but not on your clients, all logins will fail.

See Also: “Framed-Compression (13)” on page 4-146.

Ascend-Maximum-Call-Duration (125)

Description: Specifies the maximum number of minutes that the TAOS unit allows individual channels in a call to stay connected, regardless of the data traffic over the connection. When the time expires in single-channel calls, the TAOS unit disconnects the call. When the time expires for a channel in a multichannel call, the TAOS unit disconnects only the single channel, leaving the call connected.

Usage: Specify an integer from 0 to 1440. The TAOS unit checks the connection once per minute, so the actual time the call is connected is slightly longer than the actual time you set. The default value is 0 (zero), which specifies that the TAOS unit does not set a limit on the duration of the call.

Example: The following user profile specifies that the TAOS unit allows individual channels in a call to stay connected for two hours, regardless of the data traffic over the connection:

```
smith User-Password="xyzzy"
   Service-Type=Login-User,
   Login-Service=Telnet,
   Login-IP-Host=10.10.10.1,
   Ascend-TS-Idle-Mode=TS-Idle-Input,
   Ascend-TS-Idle-Limit=60,
   Ascend-Maximum-Call-Duration=120
```

Dependencies: For single-channel calls, the functionality of Session-Timeout matches the functionality of Ascend-Maximum-Call-Duration.

See Also: "Session-Timeout (27)" on page 4-160.

Ascend-Maximum-Channels (235)

Description: Specifies the maximum number of channels allowed on an MP+ call.

Usage: Specify an integer from 1 to the maximum number of channels your system supports. The default value is 1, which prevents a client from establishing a multichannel call.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Maximum-Channels:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: The Ascend-Maximum-Channels attribute applies only to MP+ calls.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Menu-Item (206)

Description: Defines a single terminal-server menu item for a user profile. You can specify up to 20 Ascend-Menu-Item attributes per profile. The screen displays the menu items in the order in which they appear in the RADIUS profile.

Using the Ascend-Menu-Item attribute, you can configure a profile to give a terminal-server user a custom menu of items from which to choose. The server uses the custom menu to present the user with a subset of terminal-server commands. The user does not have access to the regular menu or to the terminal-server command line.

Usage: Enter your specifications using the following format:

`Ascend-Menu Item=`*`command;text;match`*

Table 4-15 lists each argument. If any entry consists of an option containing more than the maximum number of characters allowed, the RADIUS server discards the entry.

Table 4-15. Ascend-Menu-Item arguments

Argument	Description
command	Specifies the string sent to the terminal server when the user selects the menu item. The string must be in a format that the terminal server understands. It can contain up to 80 characters.
text	Specifies the text that appears on the user's screen, up to 31 characters.
match	Specifies the pattern, of up to 10 characters, that the user must type to select the item. The TAOS unit considers blanks part of the matching pattern.
; (semi-colon)	The first semicolon (;) you enter acts as the delimiter between *command* and *text*. If you enter a second semicolon, it acts as the delimiter between *text* and *match*.

By default, the TAOS unit uses the standard terminal-server menu.

Example: Suppose you set the following attributes:

```
Emma User-Password="m2dan", Service-Type=Login-User
   Ascend-Menu-Item="show ip stats;Display IP Stats",
   Ascend-Menu-Item="ping 1.2.3.4;Ping server",
   Ascend-Menu-Item="telnet 10.2.4.5; Telnet to Ken's machine",
   Ascend-Menu-Item="show arp;Display ARP Table"
   Ascend-Menu-Selector="              Option:"
```

The terminal server displays the following text:

```
1. Display IP Stats     3. Telnet to Ken's machine
2. Ping server          4. Display ARP Table.
               Option:
```

See Also: "Ascend-Menu-Selector (205)" on page 4-103.

Ascend-Menu-Selector (205)

Description: Specifies a string as a prompt for user input in the terminal-server menu interface. By default, when you create a custom menu with the Ascend-Menu-Item attribute, the terminal server displays the following string when prompting the user to make a selection:

```
Enter Selection (1-num, q)
```

The *num* argument represents the last number in the list. The terminal server automatically determines the value of *num* by counting the number of items in the menu. The only valid user input is in the range 1 through *num*, and q to quit. However, you can specify a different string for prompting the user to make a selection. The Ascend-Menu-Selector attribute enables you to specify a string that the terminal server displays when prompting a user for a menu selection.

Usage: Specify a text string of up to 31 characters. The terminal server displays the string when prompting the user for a menu selection.

Example: Suppose you set the following attributes:

```
Emma User-Password="m2dan", Service-Type=Login-User
   Ascend-Menu-Item="show ip stats;Display IP Stats",
   Ascend-Menu-Item="ping 1.2.3.4;Ping server",
   Ascend-Menu-Item="telnet 10.2.4.5; Telnet to Ken's machine",
   Ascend-Menu-Item="show arp;Display ARP Table"
   Ascend-Menu-Selector="              Option:"
```

The terminal server displays the following text:

```
1. Display IP Stats     3. Telnet to Ken's machine
2. Ping server          4. Display ARP Table.
               Option:
```

Note that the valid user input in this example is still 1 through 4, or q to quit.

See Also: "Ascend-Menu-Item (206)" on page 4-102.

Ascend-Metric (225)

Description: Specifies the virtual hop count of an IP route.

If there are two routes available to a single destination network, you can make sure that the TAOS unit uses any available nailed-up channel before it uses a switched channel. Simply set the Ascend-Metric attribute to a value higher than the metric of any nailed-up route. The higher the value you enter, the less likely that the TAOS unit will bring the link online. The TAOS unit uses the lowest metric.

Usage: Specify a number from 1 to 15. The default value is 7.

Example: If a route to a station takes three hops over nailed-up lines, and Ascend-Metric=4 in a user profile that reaches the same station, the TAOS unit does not bring the user's link online. However, if the link is already online, the TAOS unit does not use the nailed-up line.

Dependencies: The hop count includes the metric of each switched link in the route.

See Also: "Ascend-Route-IP (228)" on page 4-126 and "Framed-Route (22)" on page 4-151.

Ascend-Minimum-Channels (173)

Description: Specifies the minimum number of channels an MP+ call maintains.

Usage: Specify a number from 1 to 32. The default value is 1.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Minimum-Channels:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: The Ascend-Minimum-Channels attribute applies only to MP+ calls.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Remove-Seconds (241)" on page 4-124,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Modem-PortNo (120)

Description: Indicates the number of the port used for the call.

Usage: The Ascend-Modem-PortNo attribute appears in Start records, Stop records, and Checkpoint records.

Example: `Ascend-Modem-PortNo=4000`

See Also: "Ascend-Modem-ShelfNo (122)" on page 4-105
and "Ascend-Modem-SlotNo (121)" on page 4-105.

Ascend-Modem-ShelfNo (122)

Description: Indicates the number of the shelf on which the modem card is located.

Usage: The Ascend-Modem-ShelfNo attribute appears in Start records, Stop records, and Checkpoint records.

Example: `Ascend-Modem-ShelfNo=1`

See Also: "Ascend-Modem-PortNo (120)" on page 4-104 and "Ascend-Modem-SlotNo (121)" on page 4-105.

Ascend-Modem-SlotNo (121)

Description: Indicates the number of the slot in which the modem card is physically located.

Usage: The Ascend-Modem-SlotNo attribute appears in Start records, Stop records, and Checkpoint records.

Example: `Ascend-Modem-SlotNo=5`

See Also: "Ascend-Modem-PortNo (120)" on page 4-104 and "Ascend-Modem-ShelfNo (122)" on page 4-105.

Ascend-MPP-Idle-Percent (254)

Description: Specifies a percentage of bandwidth utilization below which the TAOS unit clears a single-channel MP+ call.

Usage: Specify a number from 0 to 99. The default value is 0 (zero), which causes the TAOS unit to ignore bandwidth utilization when determining whether to clear a call.

Example: The following user profile specifies that the TAOS unit clears a single-channel MP+ call when bandwidth utilization falls below ten percent:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Maximum-Call-Duration=10,
      Ascend-MPP-Idle-Percent=10
```

Dependencies: Consider the following:

- MP+ must be in use on the link.
- If either end of a connection sets the Ascend-MPP-Idle-Percent attribute to 0 (zero), the TAOS unit ignores bandwidth utilization when determining when to clear a call.
- Bandwidth utilization *on both sides of the connection* must fall below the percentage specified by Ascend-MPP-Idle-Percent before the TAOS unit clears the call.
- If the device at the remote end of the link enters an Ascend-MPP-Idle-Percent setting lower than the value you specify, the TAOS unit does not clear the call until bandwidth utilization falls below the lower percentage.
- If the time set by the Idle-Timeout expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting.

- When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Idle-Timeout attribute has expired.
- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, Lucent recommends that you use the Idle-Timeout attribute instead.

See Also: "Ascend-Preempt-Limit (245)" on page 4-114 and "Idle-Timeout (28)" on page 4-153.

Ascend-MTU (49)

Description: Specifies the maximum size (in bytes) for a PPP over Ethernet (PPPoE) packet.

Usage: Specify an integer.

Example: The following profile specifies a maximum packet size of 1524 bytes:

```
permconn-Yossi-1 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-1483,
        User-Name="b-rad-pppoe",
        Framed-Routing=None,
        Acct-Authentic=None,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-Group="2",
        Ascend-Call-Type=Nailed,
        Ascend-Route-IP=Route-IP-No,
        Ascend-Bridge=Bridge-Yes,
        Ascend-ATM-Vpi=15,
        Ascend-ATM-Vci=35,
        Ascend-Data-Svc=Nailed-64K,
        Ascend-PPPoE-Enable=PPPoE-Yes,
        Ascend-Bridge-Non-PPPoE=Bridge-Non-PPPoE-No,
        Ascend-MTU=1524
```

See Also: "Ascend-PPPoE-Enable (74)" on page 4-113.

Ascend-Multicast-Client (155)

Description: Specifies whether the user is a multicast client of the TAOS unit.

Usage: Specify one of the following values:

- Multicast-No (0) specifies that the user is not a multicast client of the TAOS unit. Multicast-No is the default.
- Multicast-Yes (1) specifies that the user is a multicast client of the TAOS unit.

Example: To set up multicast forwarding on the WAN interfaces that support multicast clients, you would set up a RADIUS user profile for each client:

```
VAT-1 User-Password="vat1", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.10,
```

```
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Multicast-Client=Multicast-Yes,
      Ascend-Multicast-GLeave-Delay=15,
      Ascend-Multicast-Rate-Limit=5

Win-1 User-Password="win1", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.11,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Multicast-Client=Multicast-Yes,
      Ascend-Multicast-GLeave-Delay=15,
      Ascend-Multicast-Rate-Limit=5

Win-2 User-Password="win2", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.12,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Multicast-Client=Multicast-Yes,
      Ascend-Multicast-GLeave-Delay=15,
      Ascend-Multicast-Rate-Limit=5
```

See Also: "Ascend-Multicast-Rate-Limit (152)" on page 4-108.

Ascend-Multicast-GLeave-Delay (111)

Description: Specifies the number of seconds the TAOS unit waits before forwarding an IGMP version 2 `leave group` message from a multicast client.

Usage: Specify a number of seconds from 0 to 120. The default is 0 (zero). If you specify a value other than the default, and the TAOS unit receives a `leave group` message, the unit sends an IGMP query to the WAN interface or client from which it received the `leave group` message. If the TAOS unit does not receive a response from an active multicast client from the same group, it sends a `leave group` message when the time you specify expires.

If you accept the default, the TAOS unit forwards a `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, set Ascend-Multicast-GLeave-Delay to a value of 10 to 20 seconds.

Example: The following RADIUS user profile specifies that the unit waits 15 seconds before forwarding a `leave group` message:

```
VAT-1 User-Password="vat1", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.10,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Multicast-Client=Multicast-Yes,
      Ascend-Multicast-GLeave-Delay=15,
      Ascend-Multicast-Rate-Limit=5
```

See Also: "Ascend-Multicast-Client (155)" on page 4-106.

Ascend-Multicast-Rate-Limit (152)

Description: Specifies how many seconds the TAOS unit waits before accepting another packet from a multicast client. To prevent multicast clients from creating response storms to multicast transmissions, you configure the user profile to limit the rate at which the TAOS unit accepts packets from clients.

Usage: Specify an integer. If you set the attribute to 0 (zero), the TAOS unit does not apply rate limiting. The default value is 100.

Example: The following user profile specifies that the unit waits five seconds before accepting another packet from the multicast client:

```
Win-1 User-Password="win1", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=11.8.9.11,
      Framed-IP-Netmask=255.255.252.0,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Multicast-Client=Multicast-Yes,
      Ascend-Multicast-GLeave-Delay=15,
      Ascend-Multicast-Rate-Limit=5
```

See Also: "Ascend-Multicast-Client (155)" on page 4-106.

Ascend-Multilink-ID (187)

Description: Specifies the ID number of the Multilink bundle when the session closes. A multilink bundle is a multichannel MP or MP+ call. In RADIUS accounting Start and Stop records, the value of Ascend-Multilink-ID is the same for all channels of a connection, including stacked channels.

Usage: Ascend-Multilink-ID is an integer value. It does not appear in a user profile and has no default value.

Example: `Ascend-Multilink-ID=64`

Dependencies: The TAOS unit sends Ascend-Multilink-ID in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Num-In-Multilink (188)" on page 4-110.

Ascend-Netware-timeout (223)

Description: Specifies how long in minutes the TAOS unit responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging connection. Responding to watchdog requests on behalf of clients is commonly called *watchdog spoofing*.

Usage: Specify an integer from 0 to 65535. The default value is 0 (zero), which allows the TAOS unit to respond to watchdog requests without a time limit. The timer begins counting down as soon as the WAN bridging link goes offline. At the end of the selected time, the TAOS

unit releases the client-server connections. If there is a reconnection of the WAN session, the TAOS unit cancels the timeout.

Example: The following profile specifies that the unit responds to watchdog requests for ten minutes:

```
ipx-unit User-Password="ascend", Service-Type=Outbound-User
         User-Name="cs",
         Ascend-Dial-Number="96135494",
         Framed-Protocol=PPP,
         Ascend-Route-IP=Route-IP-Yes,
         Framed-IP-Address=10.10.10.11,
         Framed-IP-Netmask=255.255.255.255,
         Framed-Routing=None,
         Ascend-Bridge=Bridge-No,
         Ascend-Route-IPX=Route-IPX-Yes,
         Ascend-IPX-Peer-Mode=IPX-Peer-Router,
         Framed-IPX-Network=109255736,
         Ascend-IPX-Alias=0,
         Ascend-Netware-timeout=10,
         Ascend-Send-Auth=Send-Auth-None,
         Ascend-Link-Compression=Link-Comp-None,
         Ascend-Metric=2
```

Dependencies: Ascend-Netware-timeout applies to IPX bridging connections when the TAOS unit is on the server LAN and not on the client LAN—that is, when Ascend-Handle-IPX=Handle-IPX-Server.

See Also: "Ascend-Handle-IPX (222)" on page 4-86.

Ascend-Numbering-Plan-ID (105)

Description: Specifies the NumberPlanID field in the called party's information element.

Usage: Ask your T1 PRI provider for information about when to use each of the following settings:

- Unknown-Numbering-Plan (0) specifies that NumberPlanID=0.
- ISDN-Numbering-Plan (1) specifies that NumberPlanID=1. ISDN-Numbering-Plan is the default.
- Private-Numbering-Plan (9) specifies that NumberPlanID=9.

Example: The following profile specifies the ISDN numbering plan:

```
dialout1 User-Password="ascend", Service-Type=Outbound-User
         User-Name="dialout1",
         Ascend-Dial-Number=857870,
         Framed-Protocol=PPP,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-Metric=2,
         Ascend-PRI-Number-Type=Abbrev-Number,
         Ascend-Numbering-Plan-ID=ISDN-Numbering-Plan,
         Ascend-Send-Auth=Send-Auth-None
```

See Also: "Called-Station-Id (30)" on page 4-144.

Ascend-Number-Sessions (202)

Description: Indicates the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.

Usage: The Ascend-Number-Sessions attribute has a compound value. The first part specifies a user-session class. The second part reports the number of active sessions in that class.

Example: Suppose that the TAOS unit has three classes of clients: Class-1, Class-2, and Class-3. At the time of the sessions report, there are eight active sessions: three Class-1 sessions, four Class-2 sessions, and one Class-3 session. The accounting packet the TAOS unit sends back to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of the class/session pairs.

Dependencies: The TAOS unit sends the Ascend-Number-Sessions attribute in an Ascend-Access-Event-Request (33) packet. Only RADIUS daemons you customize to recognize this packet respond to requests from the TAOS unit. Other daemons ignore it.

When modifying the daemon, make sure that it recognizes an Ascend-Access-Event-Request packet in the following format:

Code (8-bit)=33
Identifier (8-bit)
Length (16-bit)
Authenticator (48-bit for an accounting server, 64-bit for an authentication server)
List of attributes

See Also: "Ascend-Event-Type (150)" on page 4-70 and "Class (25)" on page 4-145.

Ascend-Num-In-Multilink (188)

Description: Indicates the number of sessions remaining in a Multilink bundle when the session closes, starting with 1. A Multilink bundle is a multichannel MP or MP+ call. The Ascend-Num-In-Multilink value shows the number of channels currently connected, including stacked channels.

Usage: Ascend-Num-In-Multilink does not appear in a user profile and has no default value.

Example: `Ascend-Num-In-Multilink=1`

Dependencies: The TAOS unit sends Ascend-Num-In-Multilink in both Start and Stop packets. The attribute appears in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Multilink-ID (187)" on page 4-108.

Ascend-Owner-IP-Addr (86)

Description: Specifies the IP address of the TAOS unit that owns the Multilink bundle.

Usage: Ascend-Owner-IP-Addr does not appear in a user profile and has no default value.

Example: `Ascend-Owner-IP-Addr=10.1.2.3`

See Also: "Ascend-Multilink-ID (187)" on page 4-108.

Ascend-Port-Redir-Portnum (83)

Description: Specifies the destination port number for IP packets that must be redirected to the IP address specified by Ascend-Port-Redir-Server.

Usage: Specify an integer. For HTTP-based traffic, specify 80.

Example: The following user profile specifies port 80:

```
atcp50 User-Password="test"
   Service-Type=Framed-User,
   Framed-Protocol=MPP,
   Framed-IP-Address=2.2.2.2,
   Framed-IP-Netmask=255.255.255.255,
   Ascend-Port-Redir-Protocol=Ascend-Proto-TCP,
   Ascend-Port-Redir-Portnum=80,
   Ascend-Port-Redir-Server=1.1.1.1
```

See Also: "Ascend-Port-Redir-Protocol (82)" on page 4-111 and "Ascend-Port-Redir-Server (84)" on page 4-112.

Ascend-Port-Redir-Protocol (82)

Description: Specifies the type of protocol associated with IP packets that must be redirected to the IP address specified by Ascend-Port-Redir-Server.

Usage: Specify one of the following values:

- Ascend-Proto-TCP (6) specifies that TCP packets must be redirected to the IP address specified by Ascend-Port-Redir-Server.
- Ascend-Proto-UDP (17) specifies that UDP packets must be redirected to the IP address specified by Ascend-Port-Redir-Server.

Example: The following user profile specifies that TCP packets must be redirected to the server at IP address 1.1.1.1:

```
atcp50 User-Password="test"
   Service-Type=Framed-User,
   Framed-Protocol=MPP,
   Framed-IP-Address=2.2.2.2,
   Framed-IP-Netmask=255.255.255.255,
   Ascend-Port-Redir-Protocol=Ascend-Proto-TCP,
   Ascend-Port-Redir-Portnum=80,
   Ascend-Port-Redir-Server=1.1.1.1
```

See Also: "Ascend-Port-Redir-Portnum (83)" on page 4-111 and "Ascend-Port-Redir-Server (84)" on page 4-112.

Ascend-Port-Redir-Server (84)

Description: Specifies the IP address to which IP packets for the connection must be redirected.

Usage: Specify an IP address in dotted decimal notation.

Example: The following user profile specifies that TCP packets must be redirected to the server at IP address 1.1.1.1:

```
atcp50 User-Password="test"
   Service-Type=Framed-User,
   Framed-Protocol=MPP,
   Framed-IP-Address=2.2.2.2,
   Framed-IP-Netmask=255.255.255.255,
   Ascend-Port-Redir-Protocol=Ascend-Proto-TCP,
   Ascend-Port-Redir-Portnum=80,
   Ascend-Port-Redir-Server=1.1.1.1
```

See Also: "Ascend-Port-Redir-Portnum (83)" on page 4-111 and "Ascend-Port-Redir-Protocol (82)" on page 4-111.

Ascend-PPP-Address (253)

Description: Specifies the IP address of the local numbered interface.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

Example: The following RADIUS user profile specifies an IP address of 10.9.1.212 for the local numbered interface:

```
numbered User-Password="localpw"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-IP-Address=10.9.1.213,
   Framed-IP-Netmask=255.255.255.252,
   Ascend-PPP-Address=10.9.1.212,
   Ascend-IF-Netmask=255.255.255.252
```

See Also: "Ascend-IF-Netmask (153)" on page 4-90 and "Ascend-Remote-Addr (154)" on page 4-123.

Ascend-PPP-Async-Map (212)

Description: Specifies the async control character map for the PPP, MP, or MP+ session. The TAOS unit passes the control characters through the link as data. Only applications running over the link use the characters.

Usage: Specify a four-byte bitmap to one or more control characters. The async control character map is defined in RFC 1548 and specifies that each bit position represents its ASCII equivalent. The bits are ordered with the lowest bit of the lowest byte being 0. For example, bit 19 corresponds to Control-S (DC3) or ASCII 19.

Example: Your specification might look like the following:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Ascend-PPP-Async-Map=19,
     Framed-Protocol=PPP,
     Framed-IP-Address=200.0.5.1,
     Framed-IP-Netmask=255.255.255.0
```

The number 19 translates to 13 hexadecimal or 10011 binary. Therefore, NUL (00), SOH (01), and EOT (04) are mapped.

Ascend-PPPoE-Enable (74)

Description: Enables or disables PPP over Ethernet (PPPoE) for the connection.

Usage: Specify one of the following settings:

- PPPoE-No (0) disables PPPoE.
- PPPoE-Yes (1) enables PPPoE.

Example: The following profile specifies that PPPoE is enabled for the connection:

```
permconn-Yossi-1 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-1483,
        User-Name="b-rad-pppoe",
        Framed-Routing=None,
        Acct-Authentic=None,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-Group="2",
        Ascend-Call-Type=Nailed,
        Ascend-Route-IP=Route-IP-No,
        Ascend-Bridge=Bridge-Yes,
        Ascend-ATM-Vpi=15,
        Ascend-ATM-Vci=35,
        Ascend-Data-Svc=Nailed-64K,
        Ascend-PPPoE-Enable=PPPoE-Yes,
        Ascend-Bridge-Non-PPPoE=Bridge-Non-PPPoE-No
```

Dependencies: For PPPoE to be enabled, bridging must be enabled as well.

See Also: “Ascend-Bridge-Non-PPPoE (75)” on page 4-24.

Ascend-PPP-VJ-1172 (211)

Description: Specifies whether the TAOS unit uses the 0037h value for the VJ compression type. The TAOS unit uses the value only during IPNCP negotiation.

RFC 1172 section 5.2 contains an erroneous statement that the VJ compression type value is 0037h. It should be 002dh. However, many older implementations use the 0037h value when negotiating VJ compression. If you do not specify a value for Ascend-PPP-VJ-1172, the VJ compression type is 002dh.

Usage: Enter your specification in the following format:

```
Ascend-PPP-VJ-1172=PPP-VJ-1172
```

Example: The following user profile specifies VJ compression type 0037h:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Framed-IP-Netmask=255.255.255.248,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-PPP-VJ-1172=PPP-VJ-1172,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2
```

See Also: "Ascend-PPP-VJ-Slot-Comp (210)" on page 4-114.

Ascend-PPP-VJ-Slot-Comp (210)

Description: Instructs the TAOS unit to not use slot compression when sending VJ-compressed packets.

When you turn on VJ compression, the TAOS unit removes the TCP/IP header, and associates a TCP/IP packet with a connection by giving it a slot ID. The first packet coming into a connection must have a slot ID, but succeeding packets need not have one. If the packet does not have a slot ID, the TAOS unit associates it with the last-used slot ID. This scenario uses slot ID compression, because the slot ID does not appear in any packet but the first in a stream.

There may be times when you want each VJ-compressed packet to have a slot ID. The Ascend-PPP-VJ-Slot-Comp attribute exists for this purpose.

Usage: To specify that no slot compression occurs, set the Ascend-PPP-VJ-Slot-Comp attribute to VJ-Slot-Comp-No (1). If you do not specify a value for Ascend-PPP-VJ-Slot-Comp, and Framed-Compression=Van-Jacobson-TCP-IP, slot compression occurs.

Example: The following user profile specifies that VJ slot compression does not occur:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Framed-IP-Netmask=255.255.255.248,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-PPP-VJ-Slot-Comp=VJ-Slot-Comp-No,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2
```

See Also: "Framed-Compression (13)" on page 4-146.

Ascend-Preempt-Limit (245)

Description: Specifies the number of idle seconds the TAOS unit waits before using one of the channels of an idle link for a new call.

Usage: Specify a number from 0 to 65535. The TAOS unit never preempts a call if you enter 0 (zero). The default value is 60.

Example: The following user profile specifies that the unit waits for two minutes before using one of the channels of an idle link for a new call:

```
John  User-Password="4yr66",Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP=Netmask=255.255.255.0,
      Ascend-Maximum-Call-Duration=10,
      Ascend-Preempt-Limit=120
```

Dependencies: The Ascend-Preempt-Limit attribute does not apply to nailed-up links.

See Also: "Ascend-MPP-Idle-Percent (254)" on page 4-105 and "Idle-Timeout (28)" on page 4-153.

Ascend-Pre-Input-Octets (190)

Description: Reports the number of octets received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Ascend-Pre-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-Pre-Input-Octets=174`

Dependencies: The TAOS unit includes Ascend-Pre-Input-Octets in an Accounting-Request packet when all of the following conditions are true:

- The session was authenticated.
- The connection was asynchronous.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Pre-Output-Octets (191)" on page 4-116.

Ascend-Pre-Input-Packets (192)

Description: Reports the number of packets received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Ascend-Pre-Input-Packets does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-Pre-Input-Packets=7`

Dependencies: The TAOS unit includes Ascend-Pre-Input-Packets in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Pre-Output-Packets (193)" on page 4-116.

Ascend-Pre-Output-Octets (191)

Description: Reports the number of octets transmitted before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Ascend-Pre-Output-Octets does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-Pre-Output-Octets=8`

Dependencies: The TAOS unit includes Ascend-Pre-Output-Octets in an Accounting-Request packet when all of the following conditions are true:

- The session was authenticated.
- The connection was asynchronous.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Pre-Input-Octets (190)" on page 4-115.

Ascend-Pre-Output-Packets (193)

Description: Reports the number of packets transmitted before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Ascend-Pre-Output-Packets does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-Pre-Output-Packets=8`

Dependencies: The TAOS unit includes Ascend-Pre-Output-Packets in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Pre-Input-Packets (192)" on page 4-115.

Ascend-PreSession-Time (198)

Description: Reports the length of time in seconds from when a call connected to when it completes authentication.

Usage: Ascend-PreSession-Time does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-PreSession-Time=10`

Dependencies: The TAOS unit includes Ascend-PreSession-Time in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

See Also: "Acct-Session-Time (46)" on page 4-5.

Ascend-PRI-Number-Type (226)

Description: Specifies the type of phone number the TAOS unit dials.

Usage: Specify one of the settings listed in Table 4-16.

Table 4-16. Ascend-PRI-Number-Type settings

Setting	Specifies
Unknown-Number (0)	Any type of number.
Intl-Number (1)	A number outside the U.S.
National-Number (2)	A number inside the U.S.
Net-Specific-Number (3)	The dialed network interprets the phone number. This setting uses TypeOfNumber=3 in the called party's Information Element.
Local-Number (4)	A number within your Centrex group.
Abbrev-Number (5)	An abbreviated phone number.

Example: In the following pseudo-user profile, a number inside the U.S. is dialed:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
     User-Name="Homer",
     Ascend-Dial-Number=555-3131,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.0.100.1,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Billing-Number=555-5555
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

See Also: "Ascend-Dial-Number (227)" on page 4-57.

Ascend-Private-Route (104)

Description: Specifies a destination address and next-hop router address for a private route.

A RADIUS user profile can specify a list of private routes associated with the connection. The private routes affect only packets received from the connection. (The routes are not added to the global routing table.) If a destination is not found in the list of private routes and there is no default private route, the global routing table is consulted for a decision on routing the packets. Otherwise, only the private routing table is consulted.

Usage: In a user profile, specify the attribute in the following format:

`Ascend-Private-Route="`*`dest_addr/netmask next_hop/netmask`*`"`

where *dest_addr/netmask* is the destination address of the route, and *next_hop/netmask* is the address of the next-hop router.

Example: Following is a sample user profile that creates three private routes associated with the caller:

```
unit50 User-Password="ascend", Service-Type=Framed-User
   Framed-Protocol=PPP,
   Framed-IP-Address=10.1.1.1,
   Framed-IP-Netmask=255.0.0.0,
   Ascend-Private-Route="170.1.0.0/16 10.10.10.1"
   Ascend-Private-Route="200.1.1.1/32 10.10.10.2"
   Ascend-Private-Route="20.1.0.0/16 10.10.10.3"
   Ascend-Private-Route="0.0.0.0/0 10.10.10.4"
```

With this profile, the private routing table for the connection contains the following routes, including a default route:

```
Dest/Mask        Gateway
170.1.0.0/16     10.10.10.1
200.1.1.1/32     10.10.10.2
20.1.0.0/16      10.10.10.3
0.0.0.0/0        10.10.10.4
```

See Also: "Ascend-Private-Route-Required (55)" on page 4-118.

Ascend-Private-Route-Required (55)

Description: Specifies whether a connection can be established if its associated private-route profile is not found.

Usage: Specify one of the following values:

- Required-No (0) specifies that the connection cannot be established if its associated private-route profile is not found.
- Required-Yes (1) specifies that the connection can be established even if its associated private-route profile is not found.

Example: The following user profile specifies that the unit disconnects the call if the private table is not found:

```
pat User-Password="my-password"
    Service-Type=Framed-User
    Framed-Protocol=PPP
    Framed-IP-Address=10.1.1.1
    Framed-IP-Netmask=255.0.0.0
    Ascend-Private-Route-Table-ID="check"
    Ascend-Private-Route-Required=Required-Yes
```

Dependencies: If you use the local configuration interface to specify that a private-route profile is required, the Ascend-Private-Route-Required value overrides the local setting.

See Also: "Ascend-Private-Route-Table-ID (54)" on page 4-119.

Ascend-Private-Route-Table-ID (54)

Description: Specifies the name of the private-route profile associated with the connection. This table can be specified in RADIUS or stored in NVRAM.

Usage: Specify a text string.

Example: The following user profile specifies a private-route profile called `check`:

```
pat User-Password="my-password"
    Service-Type=Framed-User
    Framed-Protocol=PPP
    Framed-IP-Address=10.1.1.1
    Framed-IP-Netmask=255.0.0.0
    Ascend-Private-Route-Table-ID="check"
    Ascend-Private-Route-Required=Required-Yes
```

See Also: "Ascend-Private-Route-Required (55)" on page 4-118.

Ascend-PW-Expiration (21)

Description: Specifies an expiration date for a user's password. When the TAOS unit makes an authentication request, the RADIUS server checks the current date against the value of Ascend-PW-Expiration. If the date of the authentication request is the same or a later date than the value of Ascend-PW-Expiration, the user receives a message saying that the password has expired.

Note: Whether password expiration occurs on the same date as Ascend-PW-Expiration or a later date depends on the functionality of your RADIUS server.

You must specify Ascend-PW-Expiration when you first create a user, and it must appear on the first line of the user profile. If it appears after the first line, RADIUS does not check the expiration date and could accept an expired password.

Usage: Specify a month, day, and year in the following format:

`month day year`

Separate each part of the date specification with one or more spaces, tabs, or commas. The default value is 00/00/00.

Table 4-17 lists each argument.

Table 4-17. Ascend-PW-Expiration arguments

Argument	Specifies
`month`	The first three letters of the month in which you want the password to expire, or the entire name of the month. Begin the specification with a capital letter.
`day`	One or more digits indicating a valid day of the month. The settings 2, 02, 002, and 0021 are all valid, but 32 is not.
`year`	A four-digit year.

Example: You might enter a specification like the following:

```
Emma User-Password="m2dan", Ascend-PW-Expiration="November 1, 1999"
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Framed-IP-Netmask=255.255.255.248,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2
```

Dependencies: Consider the following:

- If a password expires and the user resets it, the RADIUS server adds the value of Ascend-PW-Lifetime to the date on which the user resets the password. The resulting date becomes the new value for Ascend-PW-Expiration.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.

See Also: "Ascend-PW-Lifetime (208)" on page 4-120.

Ascend-PW-Lifetime (208)

Description: Specifies the number of days that a password is valid.

Usage: Specify an integer. You can set the Ascend-PW-Lifetime attribute on any line other than the first.

Example: You might make the following specification:

```
Emma User-Password="m2dan", Ascend-PW-Expiration="November 1, 1999"
     Ascend-PW-Lifetime=30,
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Framed-IP-Netmask=255.255.255.248,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2
```

Dependencies: Consider the following:

- If a password expires and the user resets it, the RADIUS server adds the value of Ascend-PW-Lifetime to the date on which the user resets the password. The resulting date becomes the new value for Ascend-PW-Expiration.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.
- If Ascend-PW-Lifetime is absent, the value of Lifetime-In-Days determines the password duration. The Lifetime-In-Days value in the RADIUS dictionary is the default value for Ascend-PW-Lifetime. By default, Lifetime-In-Days is 0 (zero), which indicates that passwords do not expire.

See Also: "Ascend-PW-Expiration (21)" on page 4-119.

Ascend-PW-Warntime (207)

Description: Specifies the number of days before password expiration that the RADIUS server sends a message informing the user that the password will expire. The message appears

when the user establishes a connection, and is carried to the TAOS unit in the Reply-Message attribute.

Usage: Specify an integer. The default is 0 (zero), which indicates that no warning message is sent.

Example: Suppose you set Ascend-PW-Warntime=5. Starting five days before the expiration of the password, the RADIUS server sends a message telling the user the number of days until the password expires.

Dependencies: Note that the user might never see a warning message, even though the RADIUS server returns the message to the TAOS unit. This situation can occur if the user is using PPP for authentication (rather than the terminal server) or using a script to exchange information with the terminal server.

See Also: "Ascend-PW-Expiration (21)" on page 4-119 and "Ascend-PW-Lifetime (208)" on page 4-120.

Ascend-QOS-Downstream (60)

Description: Specifies the contract name for downstream traffic.

Usage: Specify a string of up to 30 characters.

Example: The following profile specifies `qos2` as the contract name for downstream traffic:

```
permconn-ST100-2 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-CIR,
        User-Name="James",
        Ascend-ATM-Group=225,
        Ascend-Route-IP=Route-IP-No,
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=33,
        Ascend-ATM-Connect-Vpi=0,
        Ascend-ATM-Connect-Vci=200,
        Ascend-ATM-Connect-Group=200,
        Ascend-QOS-Upstream="qos1",
        Ascend-QOS-Downstream="qos2"
```

See Also: "Ascend-QOS-Upstream (59)" on page 4-121.

Ascend-QOS-Upstream (59)

Description: Specifies the contract name for upstream traffic.

Usage: Specify a string of up to 30 characters.

Example: The following profile specifies `qos1` as the contract name for upstream traffic:

```
permconn-ST100-2 User-Password="ascend"
        Service-Type=Outbound-User,
        Framed-Protocol=ATM-CIR,
        User-Name="James",
        Ascend-ATM-Group=225,
```

```
        Ascend-Route-IP=Route-IP-No,
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=33,
        Ascend-ATM-Connect-Vpi=0,
        Ascend-ATM-Connect-Vci=200,
        Ascend-ATM-Connect-Group=200,
        Ascend-QOS-Upstream="qos1",
        Ascend-QOS-Downstream="qos2"
```

See Also: "Ascend-QOS-Downstream (60)" on page 4-121.

Ascend-Receive-Secret (215)

Description: Specifies a value that must match the password the calling unit sends to your TAOS unit.

Usage: Specify up to 20 characters. The default value is null.

Example: The following example shows the settings you would specify for a user called Emma to access an Enigma Logic server. Because the profile includes Ascend-Receive-Secret, the TAOS unit can authenticate additional channels through CHAP without having to use the SAFEWORD server for authentication.

```
Emma  User-Password="SAFEWORD", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Receive-Secret="b5XSAM"
```

Dependencies: You can set the Ascend-Receive-Secret attribute for Cache-Token or PAP-Token-CHAP authentication only.

See Also: "Ascend-Send-Secret (214)" on page 4-131.

Ascend-Recv-Name (45)

Description: Specifies the PPP called device's name during outgoing calls. Because bidirectional authentication provides a way to formally authenticate the called device during an outgoing call, the name of the device must be checked against a locally defined name. The name can be the dialout profile name, or a substituted name.

Usage: Specify a string of up to 23 characters.

Example: Consider the following first-tier dialout profile, configured for bidirectional CHAP authentication:

```
user1-CA-out User-Password="ascend"
     Service-Type=Outbound-User,
     Framed-Protocol=PPP,
     Framed-IP-Address=10.4.8.8,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Dial-Number=90492386067,
     Ascend-Data-Svc=Switched-64K,
     Ascend-Send-Auth=Send-Auth-CHAP,
     Ascend-Send-Secret="passin",
```

```
Ascend-Bi-Directional-Auth=Bi-Directional-Auth-Required,
Ascend-Recv-Name="user1-CA",
Ascend-Route-IP=1
```

To enforce the second RADIUS lookup, the dialout profile name (`user1-CA-out` in this example) must be different from the name of the called device in the user profile. The Ascend-Recv-Name attribute specifies the name of the called device, in this case `user1-CA`. In the following second-tier user profile, the called party's name is `user1-CA` and the receive-password is `pass`.

```
user1-CA User-Password="pass"
         Service-Type=Framed-User
         Ascend-Route-IP=1"
```

Dependencies: Consider the following:

- The value you specify for Ascend-Recv-Name is used only during outgoing calls that use bidirectional authentication.
- If you accept the default of null for Ascend-Recv-Name, the name of the called device is checked against the dialout profile name.
- Because Ascend-Recv-Name represents the called device's real name, it is sent in RADIUS accounting Start and Stop messages.

See Also: "Ascend-Bi-Directional-Auth (46)" on page 4-19.

Ascend-Redirect-Number (109)

Description: Indicates the redirected number extracted from the Redirect Number Information Element (IE) in an ISDN frame. If the IE is present, this number is sent to the RADIUS server for each Start and Stop accounting request. If the IE is not present in the frame, the attribute is not sent to the RADIUS server

Usage: You can use the Redirect Number Information Element in an ISDN frame to bill dial-in clients according to the original called number. This Information Element is generated by a Public Switched Telephone Network (PSTN) switch when the phone number dialed by a customer has been redirected to an another number.

Example: `Ascend-Redirect-Number="8005555555"`

See Also: "Called-Station-Id (30)" on page 4-144.

Ascend-Remote-Addr (154)

Description: Specifies the IP address of the numbered interface at the remote end of a link.

Usage: Specify the IP address of the numbered interface in dotted decimal notation. The default value is 0.0.0.0.

Example: The following user profile specifies IP address 2.20.20.1 for the numbered interface at the remote end of the connection:

```
tgt1 User-Password="ascend",
       Service-Type=Framed-User,
       Ascend-Data-Svc=Switched-64K,
       Ascend-Dial-Number="76969",
```

```
User-Name=tgt1,
Ascend-Send-Auth=Send-Auth-PAP,
Ascend-Send-Passwd="ascend",
Ascend-Authen-Alias="calr1" ,
Ascend-Callback=Callback-Yes,
Ascend-Callback-Delay=5,
Framed-Protocol=PPP,
Framed-Route="4.4.4.1/32 2.20.20.1 1 n",
Ascend-PPP-Address=2.30.30.1,
Ascend-IF-Netmask=255.255.255.255,
Ascend-Remote-Addr=2.20.20.1,
Ascend-Route-IP=Route-IP-Yes
```

Dependencies: For Ascend-Remote-Addr to apply, you must enable IP for the user profile (Ascend-Route-IP=Route-IP-Yes).

See Also: "Ascend-IF-Netmask (153)" on page 4-90, "Ascend-PPP-Address (253)" on page 4-112, and "Ascend-Route-IP (228)" on page 4-126.

Ascend-Remote-FW (110)

Description: Specifies the name of a firewall to download to a remote system running the Secure Connect Personal Edition (SCPE).

Usage: Specify the name of the firewall file.

Example: `Ascend-Remote-FW="company.com"`

Dependencies: The Ascend-Remote-FW value is not sent directly to the TAOS unit. Rather, the value is used by the Ascend Remote Firewall Installer (ARFI).

See Also: "Ascend-FCP-Parameter (119)" on page 4-71.

Ascend-Remove-Seconds (241)

Description: Specifies the number of seconds that average line utilization (ALU) for transmitted data must fall below the Ascend-Target-Util threshold before the TAOS unit begins removing bandwidth from a session. The TAOS unit determines the ALU for a session by means of the Ascend-History-Weigh-Type algorithm.

When utilization falls below the threshold for a period of time greater than the value of the Ascend-Remove-Seconds attribute, the TAOS unit attempts to remove the number of channels specified by the Ascend-Dec-Channel-Count attribute. Using the Ascend-Remove-Seconds attribute prevents the system from continually subtracting bandwidth, and can slow down the process of removing bandwidth.

Usage: Specify a number from 1 to 300. The default value is 10.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Remove-Seconds:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
```

```
Framed-IP-Address=200.0.5.1,
Framed-IP-Netmask=255.255.255.0,
Ascend-Target-Util=80,
Ascend-History-Weigh-Type=History-Constant,
Ascend-Seconds-Of-History=90,
Ascend-Base-Channel-Count=2,
Ascend-Add-Seconds=30,
Ascend-Remove-Seconds=30,
Ascend-Minimum-Channels=2,
Ascend-Maximum-Channels=10,
Ascend-Inc-Channel-Count=2,
Ascend-Dec-Channel-Count=2,
Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- One channel must be up at all times.
- Removing bandwidth cannot cause the ALU to exceed the threshold specified by the Ascend-Target-Util attribute.
- The number of channels remaining cannot fall below the amount specified by the Ascend-Minimum-Channels attribute.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value. If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Seconds-Of-History (238)" on page 4-129, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Require-Auth (201)

Description: Specifies whether the TAOS unit requires additional authentication after Calling-Line ID (CLID) or called-number authentication.

Usage: Specify one of the following values:

- Not-Require-Auth (0) specifies that the TAOS unit does not require additional authentication. Not-Require-Auth is the default.
- Require-Auth (1) specifies that the TAOS unit requires additional authentication.

Example: The following example shows a two-tiered approach to using the Ascend-Require-Auth attribute. The first user profile specifies CLID authentication, and indicates that additional authentication will follow. The second user profile sets up other attributes for the call.

```
5551212   User-Password="Ascend-CLID"
          Ascend-Require-Auth=Require-Auth

Emma   User-Password="pwd", Calling-Station-Id="5551212",
Service-Type=Framed-User
       Framed-Protocol=PPP,
       Framed-IP-Address=200.11.12.10,
       Framed-IP-Netmask=255.255.255.248,
       Ascend-Send-Secret="pwd"
```

Dependencies: When you set Ascend-Require-Auth=Require-Auth, you should not include any other attributes in the user profile. You must specify the characteristics of the call in another user profile.

See Also: "Calling-Station-Id (31)" on page 4-145.

Ascend-Route-Appletalk (118)

Description: Specifies whether AppleTalk routing is allowed for the user profile.

Usage: Specify one of the following values:

- Route-AppleTalk-No (0) disables AppleTalk routing for the profile. This setting is the default.
- Route-AppleTalk-Yes (1) enables AppleTalk routing for the profile.

Example: The following user profile specifies AppleTalk routing for the connection:

```
ppp-atalk User-Password="localpw"
    Service-Type=Framed-User,
    Framed-Protocol=PPP,
    Ascend-Route-Appletalk=Route-Appletalk-Yes,
    Ascend-Appletalk-Peer-Mode=Appletalk-Peer-Dialin
```

See Also: "Ascend-ARA-PW (181)" on page 4-8.

Ascend-Route-IP (228)

Description: Specifies whether IP routing is allowed for the user profile.

Usage: Specify one of the following values:

- Route-IP-No (0) disables IP routing for the profile.
- Route-IP-Yes (1) enables IP routing for the profile. Route-IP-Yes is the default.

Example: The following user profile specifies IP routing for the connection:

```
Emma User-Password="localpw"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-IP-Address=10.9.1.213,
   Framed-IP-Netmask=255.255.255.252
```

See Also: "Framed-Route (22)" on page 4-151.

Ascend-Route-IPX (229)

Description: Specifies whether IPX routing is allowed for the user profile.

Usage: Specify one of the following values:

- Route-IPX-No (0) disables IPX routing. Route-IPX-No is the default.
- Route-IPX-Yes (1) enables IPX routing.

Example: The following user profile specifies IPX routing for the connection:

```
sitebgw User-Password="sitebpw"
   Service-Type=Framed-User,
   Framed-Protocol=MPP,
   Ascend-Route-IPX=Route-IPX-Yes,
   Ascend-IPX-Peer-Mode=IPX-Peer-Router
```

Dependencies: For PPP and MP+ calls, both ends of the connection must have matching settings to route IPX.

See Also: "Ascend-IPX-Alias (224)" on page 4-96, "Ascend-IPX-Peer-Mode (216)" on page 4-98, and "Ascend-IPX-Route (174)" on page 4-98.

Ascend-Route-Preference (126)

Description: Specifies the preference for a route defined by the Framed-IP-Address attribute in a user profile. Every RADIUS user profile that specifies an explicit IP address using the Framed-IP-Address attribute indicates a static route.

Usage: Specify an integer. The default value is 60. Lucent recommends that you accept the default.

Example: The following user profile specifies a route preference of 60 for the static route defined by Framed-IP-Address:

```
Unit1 User-Password="mypw", Service-Type=Framed-User
       Framed-Protocol=PPP,
       Framed-IP-Address=10.0.200.225,
       Framed-IP-Netmask=255.255.255.0,
       Framed-Route-Preference=60,
       Ascend-Metric=2,
       Framed-Routing=None
```

Dependencies: Make sure that more desirable routes have a lower preference number. In particular, make sure that routes for connections that are down have a higher preference number than routes for connections that are up. Table 4-18 lists the factory default values for route preferences.

Table 4-18.Route preferences

Route type	Default value
Interface	0

Table 4-18.Route preferences

Route type	Default value
ICMP	30
RIP	100
OSPF ASE	150
OSPF Internal	10
Static	60
Down-WAN	120
Infinite	225

See Also: "Framed-IP-Address (8)" on page 4-147.

Ascend-Secondary-Home-Agent (130)

Description: Specifies the secondary Home Agent the Foreign Agent tries to reach when the primary Home Agent (Tunnel-Server-Endpoint) times out, or the Foreign Agent receives an error code in an ATMP Register Reply or Challenge Request message. The attribute also specifies the UDP port the Foreign Agent uses for the link.

Usage: Specify the secondary Home Agent using the following format:

`Ascend-Secondary-Home-Agent="`*`hostname`* `|` *`ip_address`* `[:`*`udp_port`*`]"`

Table 4-19 lists each element of the syntax.

Table 4-19. Ascend-Secondary-Home-Agent syntax

Syntax element	Specifies
`hostname`	Home Agent's symbolic hostname.
`ip_address`	Home Agent's IP address in dotted decimal notation. Specify an IP address if a DNS server is not set up for the Home Agent. You can specify a host name or an IP address, but not both. The Home Agent IP address should be the system address, not the IP address of the interface on which the Home Agent receives tunneled data.
`udp_port`	UDP port on which the Foreign Agent communicates with the Home Agent. The default value is 5150.
`:` (colon)	Separator between the hostname (or IP address) and the UDP port.

Example: To specify `taos.home.com` at IP address 10.0.0.2 as the secondary Home Agent, and to indicate that the Foreign Agent should use UDP port 6002, enter one of the following lines in the RADIUS user profile:

```
Ascend-Secondary-Home-Agent="taos.home.com:6002"
```

```
Ascend-Secondary-Home-Agent="10.0.0.2:6002"
```

To specify a primary Home Agent and a secondary Home Agent, enter the following lines in the RADIUS user profile:

```
Tunnel-Server-Endpoint="taos1.home.com:6001"
```

```
Ascend-Secondary-Home-Agent="taos2.home.com:6002"
```

The Foreign Agent first tries taos1.home.com on UDP port 6001. If the name cannot be resolved, or if taos1.home.com does not respond, the Foreign Agent then tries taos2.home.com on UDP port 6002.

Dependencies: If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Ascend-Secondary-Home-Agent attribute, you need not specify a value for *udp_port*. By the same token, if you specify a value for the *udp_port* argument of Ascend-Secondary-Home-Agent, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.

See Also: "Ascend-Home-Agent-UDP-Port (186)" on page 4-89,
"Ascend-Home-Network-Name (185)" on page 4-89,
"Tunnel-Server-Endpoint (67)" on page 4-165, and
"Tunnel-Server-Endpoint (67)" on page 4-165.

Ascend-Seconds-Of-History (238)

Description: Specifies the number of seconds the TAOS unit uses as a sample for calculating average line utilization (ALU) of transmitted data. The TAOS unit arrives at this average by using the algorithm specified by the Ascend-History-Weigh-Type attribute.

Usage: Specify a number from 1 to 300. The default value is 15 seconds. The number of seconds you specify depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you might want the TAOS unit to use a longer time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you might want to specify a shorter period of time. Doing so assigns less weight to the short spikes.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Seconds-Of-History:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
```

```
Ascend-Maximum-Channels=10,
Ascend-Inc-Channel-Count=2,
Ascend-Dec-Channel-Count=2,
Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: Consider the following:

- Ascend-Seconds-Of-History applies only to MP+ calls.
- If you specify a small value for the Ascend-Seconds-Of-History attribute, and increase the values of the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes, the system becomes less responsive to quick spikes.
- The easiest way to determine the values for all the attributes is to observe usage patterns.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124, and
"Ascend-Target-Util (234)" on page 4-134.

Ascend-Send-Auth (231)

Description: Specifies the authentication protocol that the TAOS unit requests when initiating a PPP or MP+ connection. The answering side of the connection determines which authentication protocol, if any, the connection uses.

Usage: Specify one of the following values:

- Send-Auth-None (0) specifies that the TAOS unit does not request an authentication protocol for outgoing calls. Send-Auth-None is the default.
- Send-Auth-PAP (1) specifies that the TAOS unit requests Password Authentication Protocol (PAP). The TAOS unit requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. To send your password unencrypted, choose this setting.
- Send-Auth-CHAP (2) specifies that the TAOS unit requests Challenge Handshake Authentication Protocol (CHAP). The remote device must support CHAP. To send an encrypted password, choose this setting or Send-Auth-MS-CHAP.
- Send-Auth-MS-CHAP (3) specifies that the TAOS unit requests Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). The remote device must support CHAP. To send an encrypted password, choose this setting or Send-Auth-CHAP.

Example: For requesting CHAP, the profile must include values for the Ascend-Send-Auth and Ascend-Send-Secret attributes. In this example, you might configure the profile as follows:

```
TAOS-Out User-Password="ascend", Service-Type=Outbound-User
        User-Name="TAOS",
        Ascend-Send-Auth=Send-Auth-CHAP,
        Ascend-Send-Secret="passwrd1",
```

```
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-IP-Address=10.0.100.1,
        Framed-IP-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1"
```

Dependencies: Consider the following:

- Ascend-Send-Auth applies only to outgoing user profiles in RADIUS.
- The link must use PPP or MP+ encapsulation.
- If you request PAP or CHAP authentication, you must also specify a password with Ascend-Send-Secret or Ascend-Send-Passwd.
- You must set Ascend-Send-Auth=Send-Auth-None for a CBCP application.

See Also: "Ascend-Send-Passwd (232)" on page 4-131 and "Ascend-Send-Secret (214)" on page 4-131.

Ascend-Send-Passwd (232)

Description: Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is not encrypted when passed between the RADIUS server and the TAOS unit.

Usage: Specify a text string of up to 20 characters. The default value is null.

Example: The following profile specifies that the unit's password is `passwrd1`:

```
TAOS-Out User-Password="ascend", Service-Type=Outbound-User
        User-Name="TAOS",
        Ascend-Send-Auth=Send-Auth-CHAP,
        Ascend-Send-Passwd="passwrd1",
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-IP-Address=10.0.100.1,
        Framed-IP-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1"
```

Dependencies: In a user profile, you can specify either Ascend-Send-Passwd or Ascend-Send-Secret, but not both. Use Ascend-Send-Passwd only if your version of the TAOS unit does not support Ascend-Send-Secret.

See Also: "Ascend-Send-Auth (231)" on page 4-130 and "Ascend-Send-Secret (214)" on page 4-131.

Ascend-Send-Secret (214)

Description: Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is encrypted when passed between the RADIUS server and the TAOS unit.

Usage: Specify a text string of up to 20 characters. The default value is null.

Example: The following profile specifies that the unit's password is `passwrd1`:

```
TAOS-Out User-Password="ascend", Service-Type=Outbound-User
        User-Name="TAOS",
        Ascend-Send-Auth=Send-Auth-CHAP,
        Ascend-Send-Secret="passwrd1",
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-IP-Address=10.0.100.1,
        Framed-IP-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1"
```

Dependencies: In a user profile, you can specify either Ascend-Send-Passwd or Ascend-Send-Secret, but not both. Use Ascend-Send-Passwd only if your version of the TAOS unit does not support Ascend-Send-Secret.

See Also: "Ascend-Send-Auth (231)" on page 4-130 and "Ascend-Send-Passwd (232)" on page 4-131.

Ascend-Session-Svr-Key (151)

Description: Enables the TAOS unit to match a user session with a client request to perform certain operations, such as disconnecting a session or changing a session's filters.

Usage: Specify up to 16 characters. The default value is null.

Example: `Ascend-Session-Svr-Key=15`

Dependencies: Consider the following:

- The client sends Ascend-Session-Svr-Key to the RADIUS server in a Disconnect-Request or Change-Filter-Request packet when it initiates an operation.
- The Ascend-Session-Svr-Key attribute appears in a RADIUS Accounting-Start packet when a session starts.

Ascend-Shared-Profile-Enable (128)

Description: Specifies whether multiple incoming callers can share a single RADIUS user profile.

Usage: Specify one of the following settings:

- Shared-Profile-No (0) specifies that multiple incoming callers cannot share the RADIUS user profile. Shared-Profile-No is the default.
- Shared-Profile-Yes (1) specifies that multiple incoming callers can share the RADIUS user profile.

Example: The following user profile can be shared by multiple callers whose username is Emma:

```
Emma User-Password="localpw"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-IP-Address=10.9.1.213,
   Framed-IP-Netmask=255.255.255.252,
   Ascend-Shared-Profile-Enable=Shared-Profile-Yes
```

Dependencies: For the Ascend-Shared-Profile-Enable attribute to apply, you must disable shared profiles for the TAOS unit.

See Also: "User-Name (1)" on page 4-167.

Ascend-Source-Auth (103)

Description: Specifies a source IP address and associated billing code. RADIUS can look up a billing code on the basis of the source IP address of a packet. When the TAOS unit places a call on behalf of a packet with the specified source address, it also sends the associated billing code to the network switch. This feature is referred to as Source Auth. Because looking up an IP address resembles a route lookup, this feature uses some of the same mechanisms as static routes. For example, Source Auth entries are retrieved from RADIUS when the router is initialized and the Source Auth information is cached for later use.

Usage: In a user profile or pseudo-user profile, make your specification in the following format:

Ascend-Source-Auth="*address/mask – authcode*"

where *address/mask* is the source address and subnet mask, and *authcode* is the billing code conveyed to the switch when a call is placed on behalf of a packet from the given source address.

As with static routes, you can indicate the subnet mask with any desired level of specificity, and the most specific entry prevails in case of conflict. The maximum length of an *authcode* is the same as the maximum for Ascend-Billing-Number: 24 digits. The hyphen (-) delimiter is reserved for future capabilities.

Example: The following profile specifies that all addresses on the 10.150.0.0 network have the billing code 5105551212, but the particular 32-bit address 10.150.0.1 has the billing code 5105551234:

```
authcode-1 User-Password="ascend", Service-Type=Outbound-User,
    Ascend-Source-Auth="10.150.0.0/16 - 5105551212",
    Ascend-Source-Auth="10.150.0.1/32 - 5105551234"
```

When you use a profile like the one in the following example, the unit retrieves the Source Auth information from RADIUS each time it retrieves the user profile for an incoming call:

```
clarap50 User-Password="pwd" Service-Type=Framed-User,
    Ascend-Dial-Number=555-1213,
    Framed-Route="10.22.22.0/24 200.1.2.3",
    Framed-Protocol=MPP,
    Framed-IP-Address=10.156.5.40/24,
    Ascend-Source-Auth="10.156.5.40/24 - 5105551212",
    Ascend-Send-Auth=Send-Auth-PAP,
    Ascend-Send-Passwd="test"
```

See Also: “Ascend-Billing-Number (249)” on page 4-20.

Ascend-Source-IP-Check (96)

Description: Enables or disables antispoofing for the session.

Usage: Specify one of the following settings:

- Source-IP-Check-No (0) disables anti-spoofing. This setting is the default.
- Source-IP-Check-Yes (1) specifies that the system checks all packets received on this interface to ensure that the source IP address in the packets matches the far-end remote address or the address agreed upon in IPCP negotiation. If the addresses do not match, the system discards the packet.

Example: In the following RADIUS user profile, antispoofing is enabled:

```
ed-mc1-p75 User-Password="localpw", Service-Type=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.7.8.200,
    Framed-IP-Netmask=255.255.255.0,
    Ascend-Source-IP-Check=Source-IP-Check-Yes
```

See Also: “Framed-IP-Address (8)” on page 4-147.

Ascend-SVC-Enabled (17)

Description: Specifies whether the Frame Relay Switched Virtual Circuit (SVC) is enabled.

Usage: Specify one of the following values:

- Ascend-SVC-Enabled-No (0) specifies that the SVC is not enabled.
- Ascend-SVC-Enabled-Yes (1) specifies that the SVC is enabled.

Example: The following profile specifies that the SVC is enabled, and indicates its telephone number:

```
frdlink-test-1 User-Password="ascend"
   Service-Type=Outbound-User,
   Framed-Protocol=FR,
   Ascend-FR-Profile-Name="svca",
   Ascend-Call-Type=Nailed,
   Ascend-FR-Nailed-Grp=21,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
   Ascend-Data-Svc=Switched-64K,
   Ascend-SVC-Enabled=Ascend-SVC-Enabled-Yes,
   Ascend-FR-SVC-Addr="2225552222"
```

See Also: “Ascend-Ckt-Type (16)” on page 4-38.

Ascend-Target-Util (234)

Description: Specifies the percentage of bandwidth use at which the TAOS unit adds or subtracts bandwidth.

Usage: Specify a number from 0 to 100. The default value is 70. With a value of 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Example: The following user profile contains all the RADIUS attributes necessary for configuring Dynamic Bandwidth Allocation (DBA), including Ascend-Target-Util:

```
John  User-Password="4yr66", Service-Type=Framed-User
      Framed-Protocol=PPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Base-Channel-Count=2,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Minimum-Channels=2,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv
```

Dependencies: When choosing a target utilization rate, consider the following:

- Monitor how the application behaves when using different bandwidths. For example, an application might be able to use 88% of a 64-Kbps link, but only 70% of a 256-Kbps link.
- Monitor the application at different loads.
- Ascend-Target-Util applies only if the link is using MP+ encapsulation.

See Also: "Ascend-Add-Seconds (240)" on page 4-5,
"Ascend-Base-Channel-Count (172)" on page 4-18,
"Ascend-DBA-Monitor (171)" on page 4-53,
"Ascend-Dec-Channel-Count (237)" on page 4-54,
"Ascend-History-Weigh-Type (239)" on page 4-87,
"Ascend-Inc-Channel-Count (236)" on page 4-91,
"Ascend-Maximum-Channels (235)" on page 4-101,
"Ascend-Minimum-Channels (173)" on page 4-104,
"Ascend-Remove-Seconds (241)" on page 4-124, and
"Ascend-Seconds-Of-History (238)" on page 4-129.

Ascend-Telnet-Profile (91)

Description: Specifies the name of the Security or User profile to use for the authenticated Telnet session. Only RADIUS profiles that specify a value for Ascend-Telnet-Profile can be used to authenticate a Telnet login to the TAOS interface.

Usage: Specify the name of a Security or User profile.

Example: Following is a sample profile that enables Telnet access to the TAOS unit with administrator permissions:

```
admin User-Password="secret-pw"
    Service-Type=Framed-User,
    Ascend-Telnet-Profile=admin
```

See Also: “Ascend-Host-Info (252)” on page 4-90 and “Login-IP-Host (14)” on page 4-154.

Ascend-Third-Prompt (213)

Description: Indicates the value entered at the third login prompt.

Usage: The Ascend-Third-Prompt attribute can contain up to 80 characters. It does not appear in a user profile. If the user enters more than 80 characters at the third prompt, the TAOS unit truncates the input to 80. If the user does not enter any characters, the TAOS unit sets the attribute to null.

Example: `Ascend-Third-Prompt="mypw"`

See Also: “Ascend-Menu-Selector (205)” on page 4-103.

Ascend-Token-Expiry (204)

Description: Specifies the lifetime (in minutes) of a cached token.

Usage: On the first line of the user profile, specify an integer representing the number of minutes in the lifetime of the cached token. The default value is 0 (zero). If you accept the default, the TAOS unit rejects subsequent Cache-Token requests from the same user.

Example: The following example shows how to set up Cache-Token authentication with a 90-minute token cache. Notice that the Ascend-Token-Expiry attribute must appear on the first line of the profile, along with the user name and password.

```
Connor  User-Password="ACE", Ascend-Token-Expiry=90
        Ascend-Receive-Secret="shared-secret",
        Service-Type=Framed-User,
        Framed-Protocol=PPP,
        Framed-IP-Address=200.0.5.1,
        Framed-IP-Netmask=255.255.255.0
```

See Also: “Ascend-Token-Idle (199)” on page 4-136 and “Ascend-Token-Immediate (200)” on page 4-137.

Ascend-Token-Idle (199)

Description: Specifies the maximum length of time in minutes a cached token can remain alive between authentications.

Usage: On the first line of the user profile, specify an integer representing the maximum length of time in minutes that a cached token can remain alive. The default value is 0 (zero). If you accept the default, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire.

Dependencies: Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

Example: The following example shows how to set up Cache-Token authentication with a 90-minute token cache and an 80-minute idle limit. Notice that the Ascend-Token-Idle attribute must appear on the first line of the profile.

```
Jim  User-Password="ACE", Ascend-Token-Expiry=90, Ascend-Token-Idle=80
     Ascend-Receive-Secret="shared secret",
     Service-Type=Framed-User,
     Framed-Protocol=PPP,
     Framed-IP-Address=200.0.5.1,
     Framed-IP-Netmask=255.255.255.0
```

See Also: "Ascend-Token-Expiry (204)" on page 4-136 and "Ascend-Token-Immediate (200)" on page 4-137.

Ascend-Token-Immediate (200)

Description: Specifies how RADIUS treats the password it receives when the user profile specifies a token-card server. Use this attribute in an ACE or SAFEWORD user profile that contains the setting Service-Type=Login-User.

Usage: Specify one of the following values:

- Tok-Imm-No (0) specifies that the TAOS unit ignores the password it receives from the user. Choose this value for a security server that requires a user to enter a token-card challenge before the server derives a password. Tok-Imm-No is the default.
- Tok-Imm-Yes (1) specifies that the TAOS unit sends the password to the token-card server for authentication.

Dependencies: The Ascend-Token-Immediate attribute does not work with CHAP authentication.

Example: To specify that the TAOS unit must send the password it receives from the login user to the ACE server, you would configure the user profile as follows:

```
Connor  User-Password="ACE", Ascend-Token-Immediate=Tok-Imm-Yes
        Ascend-Receive-Secret="shared-secret",
        Service-Type=Login-User,
        Login-Service=TCP-Clear,
        Login-IP-Host=10.10.10.1,
        Login-TCP-Port=23
```

See Also: "Ascend-Token-Expiry (204)" on page 4-136 and "Ascend-Token-Idle (199)" on page 4-136.

Ascend-Traffic-Shaper (51)

Description: Specifies the data rate (in kbps) for transmissions over an Asynchronous Transfer Mode (ATM) link.

Usage: Specify an integer from 1 to 16.

Example: The following profile specifies a data rate of 16 kbps:

```
permconn-Yossi-1 User-Password="ascend"
         Service-Type=Outbound-User,
         Framed-Protocol=ATM-1483,
```

```
        User-Name="nailed-atm",
        Framed-Routing=None,
        Ascend-Route-IP=Route-IP-Yes,
        Framed-IP-Address=222.222.2.1,
        Framed-IP-Netmask=255.255.255.0,
        Ascend-Call-Type=Nailed,
        Ascend-Group="10",
        Ascend-ATM-Vpi=0,
        Ascend-ATM-Vci=50,
        Ascend-Traffic-Shaper=16
```

See Also: "Ascend-ATM-Connect-Group (63)" on page 4-10,
"Ascend-ATM-Connect-Vci (62)" on page 4-11,
"Ascend-ATM-Connect-Vpi (61)" on page 4-11,
"Ascend-ATM-Direct (76)" on page 4-12,
"Ascend-ATM-Direct-Profile (77)" on page 4-12,
"Ascend-ATM-Fault-Management (14)" on page 4-13,
"Ascend-ATM-Group (64)" on page 4-14,
"Ascend-ATM-Loopback-Cell-Loss (15)" on page 4-14,
"Ascend-ATM-Vci (95)" on page 4-15, and
"Ascend-ATM-Vpi (94)" on page 4-15.

Ascend-Transit-Number (251)

Description: Specifies the U.S Interexchange Carrier (IEC) you use for long-distance calls over a T1 PRI line.

Usage: Specify the same digits you use to prefix a phone number you dial over a T1 access line or voice interface:

- 288 selects AT&T.
- 222 selects MCI.
- 333 selects Sprint.

The default value is null. If you accept the default, the TAOS unit uses any available IEC for long-distance calls.

Example: The following pseudo-user profile specifies AT&T as the IEC for long-distance calls:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
     User-Name="Homer",
     Ascend-Dial-Number=555-3131,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.0.100.1,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Transit-Number=288,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

See Also: "Ascend-PRI-Number-Type (226)" on page 4-117.

Ascend-TS-Idle-Limit (169)

Description: Specifies the number of seconds that a terminal-server connection must be idle before the TAOS unit disconnects the session.

Usage: Specify a value from 0 to 65535.The default value is 120. A setting of 0 (zero) specifies that the line can be idle indefinitely.

Example: To specify that the user must be idle for 90 seconds before the TAOS unit disconnects the session, you could configure a user profile as follows:

```
Default User-Password="UNIX", Service-Type=Login-User
       Ascend-TS-Idle-Limit=90,
       Ascend-TS-Idle-Mode=TS-Idle-Input
```

Dependencies: Ascend-TS-Idle-Limit does not apply if you are using a Frame Relay or raw TCP connection, or if Ascend-TS-Idle-Mode=TS-Idle-None.

See Also: "Ascend-TS-Idle-Mode (170)" on page 4-139.

Ascend-TS-Idle-Mode (170)

Description: Specifies whether the TAOS unit uses a terminal-server idle timer and, if so, whether both the user and host must be idle before the TAOS unit disconnects the session.

Usage: Specify one of the following settings:

- TS-Idle-None (0) specifies that the TAOS unit does not disconnect the session no matter how long the line is idle. This setting disables the idle timer.
- TS-Idle-Input (1) specifies that the TAOS unit disconnects the session if the user is idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute. TS-Idle-Input is the default.
- TS-Idle-Input-Output (2) specifies that the TAOS unit disconnects the session if both the user and the host are idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

Example: The following user profile specifies that the unit disconnects the session if the user is idle for more than one minute:

```
smith User-Password="xyzzy"
   Service-Type=Login-User,
   Login-Service=Telnet,
   Login-IP-Host=10.10.10.1,
   Ascend-TS-Idle-Mode=TS-Idle-Input,
   Ascend-TS-Idle-Limit=60,
   Ascend-Maximum-Call-Duration=120
```

Dependencies: Ascend-TS-Idle-Mode does not apply if you are using a Frame Relay or raw TCP connection.

See Also: "Ascend-TS-Idle-Limit (169)" on page 4-139.

Ascend-Tunnel-VRouter-Name (31)

Description: Specifies the name of a virtual router to use for establishing a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnel.

Usage: Specify the name of a VRouter used for establishing an L2TP or L2F tunnel. The specified VRouter must exist on the TAOS unit. If you do not specify a value for Ascend-Tunnel-VRouter-Name, the unit uses the global VRouter.

Example: The following profile specifies an L2TP session that belongs to a VRouter named XYZ:

```
l2tp-vrouter User-Password="localpw"
    Service-Type=Framed-User,
    Framed-Protocol=PPP,
    Framed-IP-Address=3.1.1.1,
    Tunnel-Server-Endpoint="1.1.1.1",
    Tunnel-Type=L2TP,
    Ascend-Tunnel-VRouter-Name="XYZ"
```

Dependencies: The Ascend-Tunnel-VRouter-Name attribute supports tagging. All specified attribute sets are used.

See Also: "Ascend-VRouter-Name (102)" on page 4-143.

Ascend-User-Acct-Base (142)

Description: Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.

Usage: Specify one of the following settings:

- Base-10 (the default) specifies that the numeric base is 10.
- Base-16 specifies that the numeric base is 16.

Example: When you set Ascend-User-Acct-Base=Base-10, the TAOS unit presents a typical session ID to the accounting server in the following way:

```
"1234567890"
```

When you set Ascend-User-Acct-Base=Base-16, the TAOS unit presents the same session ID in the following way:

```
"499602D2"
```

Dependencies: Changing the value of Ascend-User-Acct-Base while sessions are active results in inconsistent reporting between the Start and Stop records.

See Also: "Ascend-User-Acct-Host (139)" on page 4-140,
"Ascend-User-Acct-Key (141)" on page 4-141,
"Ascend-User-Acct-Port (140)" on page 4-141,
"Ascend-User-Acct-Time (143)" on page 4-142, and
"Ascend-User-Acct-Type (138)" on page 4-143.

Ascend-User-Acct-Host (139)

Description: Specifies the IP address of the RADIUS accounting server for the connection.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

Example: The following user profile specifies the RADIUS accounting server at IP address 200.250.56.10:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword"
```

See Also: "Ascend-User-Acct-Base (142)" on page 4-140,
"Ascend-User-Acct-Key (141)" on page 4-141,
"Ascend-User-Acct-Port (140)" on page 4-141,
"Ascend-User-Acct-Time (143)" on page 4-142, and
"Ascend-User-Acct-Type (138)" on page 4-143.

Ascend-User-Acct-Key (141)

Description: Specifies the RADIUS client password.

Usage: Specify a text string. The default value is null.

Example: The following user profile specifies the RADIUS client password as `mypassword`:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword"
```

See Also: "Ascend-User-Acct-Base (142)" on page 4-140,
"Ascend-User-Acct-Host (139)" on page 4-140,
"Ascend-User-Acct-Port (140)" on page 4-141,
"Ascend-User-Acct-Time (143)" on page 4-142, and
"Ascend-User-Acct-Type (138)" on page 4-143.

Ascend-User-Acct-Port (140)

Description: Specifies a UDP port number for the connection between the user and the RADIUS accounting server.

Usage: Specify the UDP port number you indicated for the authentication process of the daemon. Or, if you used the `incr` keyword to the `-A` argument when starting the daemon, specify the number of the UDP port for authentication services plus 1. You can specify a number from 1 to 32767.

Example: The following user profile specifies UDP port 1645 for the connection between the user Emma and the RADIUS accounting server:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword"
```

See Also: "Ascend-User-Acct-Base (142)" on page 4-140,
"Ascend-User-Acct-Host (139)" on page 4-140,
"Ascend-User-Acct-Key (141)" on page 4-141,
"Ascend-User-Acct-Time (143)" on page 4-142, and
"Ascend-User-Acct-Type (138)" on page 4-143.

Ascend-User-Acct-Time (143)

Description: Specifies the number of seconds the TAOS unit waits for a response to a RADIUS accounting request for the connection.

Usage: Specify an integer from 1 to 10. The default value is 0 (zero).

Example: The following user profile specifies that the unit waits five seconds for a response to a RADIUS accounting request:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword",
     Ascend-User-Acct-Time=5
```

See Also: "Ascend-User-Acct-Base (142)" on page 4-140,
"Ascend-User-Acct-Host (139)" on page 4-140,
"Ascend-User-Acct-Key (141)" on page 4-141,
"Ascend-User-Acct-Port (140)" on page 4-141, and
"Ascend-User-Acct-Type (138)" on page 4-143.

Ascend-User-Acct-Type (138)

Description: Specifies the RADIUS accounting server(s) to use for the connection.

Usage: Specify one of the following settings:

- Ascend-User-Acct-None (0) specifies that the TAOS unit sends accounting information to the RADIUS server specified at the local configuration interface. This server is known as the *default server.* Ascend-User-Acct-None is the default.
- Ascend-User-Acct-User (1) specifies that the TAOS unit sends accounting information to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile.
- Ascend-User-Acct-User-Default (2) specifies that the TAOS unit sends accounting information both to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile, and to the default server.

Example: The following user profile specifies that the unit sends accounting information to the RADIUS server at 200.250.56.10:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword",
     Ascend-User-Acct-Time=5
```

See Also: "Ascend-User-Acct-Base (142)" on page 4-140,
"Ascend-User-Acct-Host (139)" on page 4-140,
"Ascend-User-Acct-Key (141)" on page 4-141,
"Ascend-User-Acct-Port (140)" on page 4-141, and
"Ascend-User-Acct-Time (143)" on page 4-142.

Ascend-VRouter-Name (102)

Description: Specifies the name of a defined Virtual Router (VRouter). Specifying the VRouter name in a RADIUS user profile groups the WAN interfaces with the VRouter.

Usage: Specify the name of a VRouter. The default is null, which specifies that the global VRouter is in use.

Example: The following user profile specifies a VRouter called Corpa:

```
bob User-Password="bob", Service-Type=Framed-User
   Framed-Protocol=PPP,
   Ascend-VRouter-Name="Corpa"
```

See Also: "Ascend-IP-Pool-Definition (217)" on page 4-93 and "Framed-Route (22)" on page 4-151.

Ascend-Xmit-Rate (255)

Description: Specifies the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the negotiated transmit modem baud rate at the time of the initial connection.

Usage: Ascend-Xmit-Rate does not appear in a user profile. Its default value is 0 (zero).

Example: `Ascend-Xmit-Rate=48000`

Dependencies: The TAOS unit sends the Ascend-Xmit-Rate attribute in Accounting-Request packets at the end of a session when the Accounting-Request packet has Acct-Status-Type=Stop. The TAOS unit sends the attribute with the Accounting-Request packet whether the unit authenticates the connection or not. The TAOS unit also includes Ascend-Xmit-Rate in an Access Request packet unless you authenticate with Calling-Line ID (CLID) or Dialed Number Information Service (DNIS).

See Also: "Ascend-Data-Rate (197)" on page 4-49.

Called-Station-Id (30)

Description: Specifies the called-party number, indicating the called number for an incoming call or an outgoing IP-Fax call. Or, specifies a VPI/VCI pair on incoming PPP over ATM calls and virtual PPPoE calls.

Usage: For a called-party number, specify a phone number, limiting your specification to the following characters:

```
1234567890()[]!z-*#|
```

You can specify up to 18 characters. The default value is null. Typically, the phone numbers different callers can use to reach the TAOS unit share a group of digits. For example, a local caller might dial 555-1234, while a long distance caller would dial 1-415-555-1234. In such cases, you need only specify the rightmost digits the calls have in common. In this example, you would specify only 1234.

For a VPI/VCI pair, specify a value in the format *vpi* | *vci*. For *vpi*, specify an integer from 0 to 255. For *vci*, specify an integer from 32 to 32767. If the user profile on the RADIUS server includes the Called-Station-Id attribute, and the value matches the one provided by the TAOS unit, the user is authenticated.

Example: To set up called-number authentication in addition to name and password authentication, you could configure the user profile as follows:

```
Clara-p50 User-Password="ascend", Called-Station-Id=1234
     Service-Type=Framed-User,
     Framed-Protocol=PPP,
     Framed-IP-Address=200.10.11.12,
     Framed-IP-Netmask=255.255.255.248
```

See Also: "Calling-Station-Id (31)" on page 4-145.

Calling-Station-Id (31)

Description: Specifies the calling-party number for Calling-Line ID (CLID) authentication, indicating the phone number of the user that wants to connect to the TAOS unit.

Usage: Specify a telephone number of up to 37 characters, limited to the following:

```
1234567890()[]!z-*#|
```

The default value is null.

Example: To set up CLID authentication with a name, password, and caller ID, you could configure a user profile as follows:

```
Emma  User-Password="test", Calling-Station-Id="123456789"
      Service-Type=Framed-User,
      Framed-Protocol=PPP,
      Framed-IP-Address=255.255.255.254,
      Framed-IP-Netmask=255.255.255.255,
      Ascend-Route-IP=Route-IP-Yes
```

See Also: "Called-Station-Id (30)" on page 4-144.

Change-Password (17)

Description: Enables the TAOS unit to change an expired password. When a user specifies an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the TAOS unit sends an Access-Password-Request packet containing both the old password (as the value of the Change-Password attribute), and the new password (as the value of the User-Password attribute).

Usage: Change-Password does not appear in a user profile and has no default value.

Example: `Change-Password="oldpw"`

See Also: "CHAP-Password (3)" on page 4-145.

CHAP-Password (3)

Description: Specifies the value that a Challenge Handshake Authentication Protocol (CHAP) user provides in response to the password challenge.

Usage: The TAOS unit sends the CHAP-Password value in an Access-Request packet. The default value is null.

Example: `CHAP-Password="xx54fhy"`

See Also: "Change-Password (17)" on page 4-145.

Class (25)

Description: Enables you to classify user sessions for purposes such as billing users on the basis of the service option they choose. Keep in mind that accounting entries specify the class on a per-user and per-session basis. The Ascend-Number-Sessions attribute reports information about all user sessions (that is, on the number of current sessions of each class).

Usage: Specify an alphanumeric text string of up to 253 characters. The default value is null.

Example: `Class="Option1"`

Dependencies: If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the TAOS unit in the Access-Accept packet when the session begins. The TAOS unit then includes Class in Accounting-Request packets it sends to the RADIUS accounting server under the following conditions:

- Whenever a session starts
- Whenever a session stops

In addition, suppose the TAOS unit starts CLID authentication by sending an Access-Request packet, and receives the Class attribute in an Access-Accept packet. If the TAOS unit requires further authentication, it includes Class in the Access-Request packet

See Also: "Ascend-Number-Sessions (202)" on page 4-110.

Filter-ID (11)

Description: Specifies the name of a local or remote filter profile associated with the connection. The next time the TAOS unit accesses the RADIUS user profile in which the Filter-ID attribute appears, the specified data filter is applied to the connection.

Usage: Specify a text string. The default is null. As is always the case with filters, the order in which they are applied within the profile is significant. If the TAOS unit supports multiple filter profiles with similar names, it uses the first filter profile to match the characters specified in the user profile.

Example: The following user profile specifies that the session uses the Filter profile called `filter-c`:

```
p50-v2 User-Password="my-password" Service-Type=Framed-User
    Framed-Protocol=PPP
    Framed-IP-Address=10.1.1.1
    Framed-IP-Netmask=255.0.0.0
    Filter-ID="filter-c"
    Ascend-Filter-Required=Required-Yes
```

Dependencies: Filter-ID does not apply to call filters or Secure Access™ Firewalls.

See Also: "Ascend-Data-Filter (242)" on page 4-45.

Framed-Compression (13)

Description: Turns TCP/IP header compression on or off.

Usage: To turn on TCP/IP header compression, specify Van-Jacobson-TCP-IP (1). This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link. By default, the Framed-Compression attribute does not turn on header compression.

Example: The following user profile specifies that TCP/IP header compression is turned on:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
```

```
Framed-IP-Address=200.250.55.9,
Framed-IP-Netmask=255.255.255.248,
Framed-Compression=Van-Jacobson-TCP-IP,
Ascend-Route-IP=Route-IP-Yes,
Ascend-Metric=2
```

Dependencies: Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

See Also: "Ascend-Link-Compression (233)" on page 4-99.

Framed-IP-Address (8)

Description: Specifies the IP address of a caller. RADIUS can authenticate an incoming caller by matching the user's IP address to the one specified in the user profile.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. An answering user profile with the default setting matches all IP addresses.

Example: The following user profile specifies the caller's IP address as 10.8.9.10:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-IP-Address=10.8.9.10,
     Framed-IP=Netmask=255.255.255.255,
     Framed-Routing=None,
     Framed-Compression=Van-Jacobson-TCP-IP
```

Dependencies: Consider the following:

- Every Connection profile and RADIUS user profile that specifies an explicit IP address is a static route.
- In a stacked configuration, Framed-IP-Address shows the address of the caller if the accounting record belongs to the bundle owner. If the accounting record belongs to a stack peer, the IP address is 0.0.0.0.

Usage: "Framed-IP-Netmask (9)" on page 4-147.

Framed-IP-Netmask (9)

Description: Specifies a subnet mask for the caller at Framed-IP-Address.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0, which specifies that the TAOS unit assumes a default subnet mask on the basis of the class of the address (as shown in Table 4-20).

Table 4-20. IP address classes and default subnet masks

Class	Address range	Network bits
Class A	0.0.0.0 -> 127.255.255.255	8

Table 4-20. IP address classes and default subnet masks (continued)

Class	Address range	Network bits
Class B	128.0.0.0 -> 191.255.255.255	16
Class C	192.0.0.0 -> 223.255.255.255	24
Class D	224.0.0.0 -> 239.255.255.255	N/A
Class E (reserved)	240.0.0.0 -> 247.255.255.255	N/A

Example: The following user profile specifies the caller's subnet mask as 255.255.255.255:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-IP-Address=10.8.9.10,
     Framed-IP=Netmask=255.255.255.255,
     Framed-Routing=None,
     Framed-Compression=Van-Jacobson-TCP-IP
```

See Also: "Framed-IP-Address (8)" on page 4-147.

Framed-IPX-Network (23)

Description: Specifies a virtual IPX network number assigned to dial-in clients to enable the Ascend Tunnel Management Protocol (ATMP) Home Agent to route IPX packets to the Mobile Client. When specified in a user profile, the Framed-IPX-Network attribute instructs the answering unit to advertise an additional IPX route.

Usage: Specify the IPX network number of the IPX router at the remote end of the connection. A value of 0xFFFFFFFE specifies that the TAOS unit should select an IPX network number from the pool that the unit maintains.

Example: The following profile specifies the IPX network number as `109255736`:

```
ipx-o User-Password="ascend", Service-Type=Outbound-User
        User-Name="cs",
        Ascend-Dial-Number="96135494",
        Framed-Protocol=PPP,
        Ascend-Route-IP=Route-IP-Yes,
        Framed-IP-Address=10.10.10.11,
        Framed-IP-Netmask=255.255.255.255,
        Framed-Routing=None,
        Ascend-Bridge=Bridge-No,
        Ascend-Route-IPX=Route-IPX-Yes,
        Ascend-IPX-Peer-Mode=IPX-Peer-Router,
        Framed-IPX-Network=109255736,
        Ascend-IPX-Alias=0,
        Ascend-Netware-timeout=10,
        Ascend-Send-Auth=Send-Auth-None,
        Ascend-Link-Compression=Link-Comp-None,
        Ascend-Metric=2
```

Dependencies: RADIUS requires that Framed-IPX-Network have a decimal value (base 10), but IPX network numbers generally appear as hexadecimal values (base 16). In order to give this attribute a value, you must convert the hexadecimal IPX network number to decimal format for use in the user profile. For example, if the IPX network number is 00001387, you must convert it to the decimal 00004999. This requirement does not apply for the IPX node address, which appears as a 12-digit string enclosed in double-quotes.

See Also: "Ascend-IPX-Node-Addr (182)" on page 4-97

Framed-MTU (12)

Description: Specifies the Maximum Transfer Unit (MTU)—the maximum number of bytes the TAOS unit can receive in a single packet on a PPP, MP, MP+, or Frame Relay link.

Usage: The default value is 1524. You should accept the default unless the device at the remote end of the link cannot support it. If the administrator of the remote network determines that you must change the value, specify a number from 1 to 1524 (for a PPP, MP, or MP+ link) or from 128 to 1600 (for a Frame Relay link).

Example: The following example specifies an MTU of 1520 bytes:

```
Emma User-Password="m2dan", Service-Type=Framed-User
     Framed-Protocol=PPP,
     Framed-IP-Address=200.250.55.9,
     Framed-IP-Netmask=255.255.255.248,
     Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Framed-MTU=1520,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2
```

Framed-Protocol (7)

Description: In an Access-Request or Access-Accept packet, specifies the type of framed protocol the link can use. In an Accounting packet, specifies the type of framed protocol in use.

Note: When you set this attribute, the link cannot use any other type of framed protocol.

Usage: Table 4-21 lists the values for Framed-Protocol. By default, the TAOS unit does not limit the protocols a link can access.

Table 4-21. Framed-Protocol settings

Setting	Description
PPP (1)	A user requesting access can dial in with Multilink Protocol Plus™ (MP+), Multilink Protocol (MP), or Point-to-Point Protocol (PPP) framing. A user requesting access can also dial in unframed, and then change to PPP, MP, or MP+ framing. If the user dials in with any other type of framing, the TAOS unit rejects the call.

Table 4-21. Framed-Protocol settings (continued)

Setting	Description
SLIP (2)	A user requesting access can dial in unframed and change to SLIP framing.
ARA (255)	Specifies an AppleTalk Remote Access (ARA) connection.
MPP (256)	Specifies Multilink Protocol Plus (MP+) encapsulation.
EURAW (257)	Specifies EU-RAW encapsulation.
EUUI (258)	Specifies EU-UI encapsulation.
X25 (259)	Specifies an X.25 link.
COMB(260)	Specifies a Combinet bridging link.
FR (261)	Specifies Frame Relay encapsulation.
MP (262)	Specifies a Multilink Protocol link.
FR-CIR (263)	Specifies a Frame Relay circuit.
ATM-1483 (264)	Specifies ATM AAL5 encapsulation (defined in RFC 1483).
ATM-FR-CIR (265)	Enables Frame Relay to ATM switching by converting Frame Relay encapsulation (defined in RFC 1490) to ATM AAL5 encapsulation (defined in RFC 1483). The conversion is described in the Frame Relay Forum FRF-5 implementation agreement.
ATM-CIR (266)	Specifies an ATM circuit.

Example: To specify that a dial-in user can only use PPP protocols (PPP, MP+, or MP), and cannot use the terminal server, you could configure a user profile as follows:

```
Unit1 User-Password="mypw", Service-Type=Framed-User
       Framed-Protocol=PPP,
       Framed-IP-Address=10.0.200.225,
       Framed-IP-Netmask=255.255.255.0,
       Ascend-Metric=2,
       Framed-Routing=None,
       Framed-Route="10.0.220.0 10.0.200.225 1"
```

Dependencies: Framed-Protocol can appear in both Access-Request and Access-Accept packets. What Framed-Protocol does depends on how you set Service-Type:

- If Service-Type=Framed-User or is unspecified, a user requesting access can dial in with the framing specified by Framed-Protocol. The TAOS unit rejects other types of framing. A user requesting access can also dial in without a framed protocol, and then change to the framing specified by Framed-Protocol.
- If Service-Type=Framed-User or is unspecified, and Framed-Protocol has no specified value, the operator can use any framed protocol.

- If Service-Type=Login-User, the user cannot use a framed protocol.
- If Service-Type=Outbound-User, Framed-Protocol specifies the type of framing allowed on the outgoing call.

When Framed-Protocol=ATM-1483 or ATM-FR-CIR, you must specify a value for Ascend-ATM-Vpi and Ascend-ATM-Vci.

See Also: "Ascend-ATM-Vci (95)" on page 4-15,
"Ascend-ATM-Vpi (94)" on page 4-15, and
"Service-Type (6)" on page 4-159.

Framed-Route (22)

Description: Enables you to add static IP routes to the TAOS unit's routing table.

Usage: The Framed-Route attribute has the following format:

`Framed-Route="host_ipaddr[/subnet_mask] gateway_ipaddr metric [private] [profile_name][preference][vrouter_name]"`

Table 4-22 describes each Framed-Route argument.

Table 4-22. Framed-Route arguments

Syntax element	Specifies
host_ipaddr [*/subnet_mask*]	IP address of the destination host or subnet reached by the route. The default value is 0.0.0.0/0., which represents the default route (the destination to which the TAOS unit forwards packets when no route to the packet's destination exists). If the address includes a subnet mask, the remote router specified by *router_ipaddr* is a router to that subnet, rather than to a whole remote network. To specify the entire remote network, do not specify a subnet mask.
router_ipaddr	IP address of the router the TAOS unit uses to reach the target destination. The default value is 0.0.0.0. The 0.0.0.0 address is a wildcard entry the TAOS unit replaces with the caller's IP address.When RADIUS authenticates a caller and sends the TAOS unit an Access-Accept message with a value of 0.0.0.0 for *router_ipaddr*, the TAOS unit updates its routing tables with the Framed-Route value, but substitutes the caller's IP address for the router. This setting is especially useful when the TAOS unit assigns an IP address from an address pool and RADIUS cannot know the IP address of the caller.
metric	Metric for the route. If the TAOS unit has more than one possible route to a destination network, it chooses the one with the lower metric. The default value is 8.

Table 4-22. Framed-Route arguments (continued)

Syntax element	Specifies
private	Value y if the route is private, or n if it is not private. If you specify that the route is private, the TAOS unit does not disclose the existence of the route when queried by RIP or another routing protocol. The default value is n.
profile_name	Name of the outgoing user profile that uses the route. The default value is null.
preference	Preference for the route.
vrouter_name	The Virtual Router (Vrouter) whose routing table will contain the static IP route.

Example: The following example shows how to set up two RADIUS pseudo-user profiles to define global static IP routes:

```
route-1   User-Password="ascend", Service-Type=Outbound-User
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n lala-gw-out ",
   Framed-Route="10.0.200.50/29 10.0.200.37 1 n lala-gw-out ",
   Framed-Route="10.0.200.47/29 10.0.200.49 1 n nana-gw-out "

route-2   User-Password="ascend", Service-Type=Outbound-User
   Framed-Route="11.0.200.33/29 11.0.200.37 1 n zzz-gw-out ",
   Framed-Route="12.0.200.47/29 11.0.200.49 1 n kk-gw-out "
```

Dependencies: The maximum number of static routes that you can specify in a pseudo-user profile is imposed by the RADIUS protocol, and varies with the exact content of the routes. However, 25 routes per profile is the recommended maximum.

See Also: "Ascend-Route-IP (228)" on page 4-126.

Framed-Routing (10)

Description: Specifies whether the TAOS unit sends Routing Information Protocol (RIP) packets, receives RIP packets, or both.

If you enable RIP to both send and receive updates on the WAN interface, the TAOS unit broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which can become quite large).

Usage: Specify one of the following values:

- None (0) specifies that the TAOS unit does not send or receive RIP updates. None is the default.
- Broadcast (1) specifies that the TAOS unit sends RIP version 1 updates, but does not receive them.
- Listen (2) specifies that the TAOS unit receives RIP version 1 updates, but does not send them.

- Broadcast-Listen (3) specifies that the TAOS unit both sends and receives RIP version 1 updates.
- Broadcast-v2 (4) specifies that the TAOS unit sends RIP version 2 updates, but does not receive them.
- Listen-v2 (5) specifies that the TAOS unit receives RIP version 2 updates, but does not send them.
- Broadcast-Listen-v2 (6) specifies that the TAOS unit both sends and receives RIP version 2 updates.

Example: The following pseudo-user profile specifies that the unit does not send or receive RIP updates:

```
Homer-Out User-Password="ascend", Service-Type=Outbound-User
     User-Name="Homer",
     Ascend-Dial-Number=555-3131,
     Framed-Protocol=MPP,
     Framed-IP-Address=10.0.100.1,
     Framed-IP-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

Dependencies: If you set Framed-Routing=None, the TAOS unit must rely on static routes you specify with Framed-Route.

See Also: "Ascend-Route-IP (228)" on page 4-126.

Idle-Timeout (28)

Description: Specifies the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.

Usage: Specify a number from 0 to 65535. If you specify 0 (zero), the TAOS unit always clears a call when a session is inactive. The default value is 120 seconds.

Example: The following user profile sets the idle timer to 60 seconds:

```
smith User-Password="xyzzy"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.0.200.225,
   Framed-IP-Netmask=255.255.255.0,
   Idle-Timeout=60,
   Ascend-Maximum-Call-Duration=120
```

Dependencies: Consider the following:

- If the time set by the Idle-Timeout expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting.
- When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Idle-Timeout attribute has expired.

- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, Lucent recommends that you use the Idle-Timeout attribute instead.
- The Idle-Timeout attribute does not apply to nailed-up link.

See Also: "Ascend-MPP-Idle-Percent (254)" on page 4-105 and "Ascend-Preempt-Limit (245)" on page 4-114.

Login-IP-Host (14)

Description: Specifies the IP host to which the user automatically connects when you:

- Set Service-Type=Login-User.
- Specify a value for Login-Service.

Access begins immediately after login.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0. 0.0, which specifies that the Login-User does not automatically connect to a particular host.

Example: The following user profile specifies a TCP-Clear connection on TCP port 23 to a host at 10.10.10.1, or on TCP port 125 to a host at 10.10.10.2:

```
tcpapp1 User-Password="localpw"
   Service-Type=Login-User,
   Login-Service=TCP-Clear,
   Login-IP-Host=10.10.10.1,
   Login-TCP-Port=23,
   Login-IP-Host =10.10.10.2,
   Login-TCP-Port=125
```

Dependencies: Consider the following:

- If you do not specify a value for the Login-IP-Host attribute, the user can access any remote host through the Telnet or raw TCP commands of the terminal-server command-line interface. (When the operator uses the menu-driven terminal-server interface, access to remote hosts is limited to the hosts listed by the Ascend-Host-Info attribute.)
- Closing the remote terminal-server session also automatically closes the session with Login-IP-Host.
- When Service-Type=Framed-User, RADIUS ignores the Login-IP-Host attribute.
- You can configure up to four login host and port destinations for a TCP-Clear connection. While the TCP-Clear session is being established, if the TCP connection to the first specified host/port combination fails, the system attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.
- TCP-Clear connections are managed on a per-router basis.

See Also: "Login-Service (15)" on page 4-155 and "Service-Type (6)" on page 4-159.

Login-Service (15)

Description: Specifies the type of terminal-server connection a dial-in user makes to the IP host on your local network. The user makes the connection immediately after authentication, and never sees the terminal-server interface.

Usage: Specify one of the following values:

- Telnet (0) specifies that the user immediately establishes a Telnet session with the host specified by Login-IP-Host.
- Rlogin (1) specifies that the user immediately establishes an Rlogin session with the host specified by Login-IP-Host.
- TCP-Clear (2) specifies that the user immediately establishes a TCP session between the TAOS unit and the host specified by Login-IP-Host. The TCP/IP connection cannot use the Telnet protocol. The user can run an application specified by Login-TCP-Port.
- PortMaster (3) specifies that the user immediately establishes a PortMaster session with the host specified by Login-IP-Host.
- X25-Pad (5) specifies that the user immediately establishes an X.25/PAD session with the host specified by Login-IP-Host.
- X25-T3Pos (6) specifies that the user immediately establishes an X.25/T3POS session with the host specified by Login-IP-Host.
- TCP-Clear-Quiet (256) enables the terminal-server software to suppress status messages sent out to IP hosts upon establishment of a TCP-Clear connection.

By default, the TAOS unit does not grant immediate access to an IP host.

Example: When you specify the following settings, a raw TCP session starts automatically for anyone who enters the Greg user name and the test1 password:

```
# The following profile causes an auto-TCP to 4.2.3.1 port 9
upon login.
Greg   User-Password="test1", Service-Type=Login-User
       Login-Service=TCP-Clear,
       Login-IP-Host=4.2.3.1,
       Login-TCP-Port=9
```

Dependencies: Consider the following:

- If you specify both Login-Service and Login-IP-Host, the TAOS unit automatically connects the Login-User to the host specified by Login-IP-Host.
- If you do not specify Login-Service or Login-IP-Host, the user sees either the TAOS unit's terminal-server command-line interface or the terminal-server menu interface, depending upon how you configure the TAOS unit.

See Also: "Login-IP-Host (14)" on page 4-154 and "Login-TCP-Port (16)" on page 4-155.

Login-TCP-Port (16)

Description: Specifies the port number to which a TCP session connects when Login-Service=TCP-Clear.

Usage: Specify an integer from 1 to 65535. The default value is 23.

Example: The following user profile specifies a TCP-Clear connection on TCP port 23 to a host at 10.10.10.1, or on TCP port 125 to a host at 10.10.10.2:

```
tcpapp1 User-Password="localpw"
   Service-Type=Login-User,
   Login-Service=TCP-Clear,
   Login-IP-Host=10.10.10.1,
   Login-TCP-Port=23,
   Login-IP-Host =10.10.10.2,
   Login-TCP-Port=125
```

Dependencies: You can configure up to four login host and port destinations for a TCP-Clear connection. While the TCP-Clear session is being established, if the TCP connection to the first specified host/port combination fails, the system attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.

See Also: "Login-IP-Host (14)" on page 4-154,
"Login-Service (15)" on page 4-155, and
"Login-TCP-Port (16)" on page 4-155.

MS-CHAP-Challenge

Description: Contains the challenge sent by the Network Access Server (NAS) to an MS-CHAP user.

Usage: The value of MS-CHAP-Challenge is a string that can appear in an Access-Request and Access-Challenge packet. For further details, refer to RFC 2548.

Example: `MS-CHAP-Challenge="ax33dk4"`

See Also: "MS-CHAP-Response" on page 4-156.

MS-CHAP-Response

Description: Contains the response value provided by a PPP MS-CHAP user in response to the challenge indicated by MS-CHAP-Challenge.

Usage: The value of MS-CHAP-Response is a string that appear only in an Access-Request packet. For further details, refer to RFC 2548.

Example: `MS-CHAP-Response="ax33dk4"`

Usage: "MS-CHAP-Challenge" on page 4-156.

NAS-IP-Address (4)

Description: Indicates the IP address of the TAOS unit.

Usage: NAS-IP-Address does not appear in a user profile. Its default value is 0.0.0.0.

Example: `NAS-IP-Address=10.10.10.10`

See Also: "NAS-Port (5)" on page 4-157.

NAS-Port (5)

Description: Indicates the network port on which the TAOS unit receives a call, or the network port from which the unit transmits an IP-Fax call. The TAOS unit sends NAS-Port to the RADIUS server in an Accounting-Request packet. If you specify NAS-Port on the first line of a user profile, the TAOS unit sends the value you specify to the RADIUS server in an Access-Request packet.

Usage: The format of the NAS-Port value depends upon whether you are using the new NAS Port format.

When using the new NAS port format

When you use the new NAS port format, the NAS-Port value has the following format:

shelf slot line channel

where *shelf* specifies the shelf number (0–3), *slot* specifies the slot number (0–15), *line* specifies the line number (0–31), and *channel* specifies the channel number (0–31) for an ISDN call. For an analog call, the values are the same, except that line number can be 0–63, and the channel number is always 1.

The values are all bit encoded. For an ISDN call, the bit-encoded number has the following format:

- The shelf number is composed of two bits.
- The slot number is composed of four bits.
- The line and channel numbers are each composed of five bits.

For an analog call, the bit-encoded number has the following format:

- The shelf number is composed of two bits.
- The slot number is composed of four bits.
- The line number is composed of six bits.
- The channel number is composed of four bits.

When using this attribute for accounting purposes, you must add 1 to each component to ascertain the actual shelf, slot, line, and channel number.

When using the old NAS port format

When you use the old NAS port format, the NAS-Port value has the following format:

tllcc

where *t* indicates 1 for a digital call or 2 for an analog call, *ll* indicates the line number, and *cc* indicates the channel number.

Example: To restrict an ISDN user to channel 2 on line 2 for slot 2 and shelf 1, you could set up a user profile as follows:

```
Robin User-Password="password", NAS-Port=1057,
Service-Type=Framed-User
      Framed-Protocol=PPP,
      Ascend-Assign-IP-Pool=1,
```

```
    Ascend-Route-IP=1,
    Framed-Routing=None
```

The NAS-Port value of 1057 translates to the bit-encoded number 0000010000100001. This number indicates the following NAS port:

shelf=00 (shelf 1)

slot=0001 (slot 2)

line=00001 (line 2)

channel=00001 (channel 2)

NAS-Port-Type (61)

Description: Specifies the type of service in use for the session. Some ISPs offer different levels of service on the basis of connection type. To prevent a client from using a capability to which he or she has not subscribed, set the NAS-Port-Type attribute to an appropriate value.

Usage: Specify one of the following settings:

- Async (0) indicates a call routed to a digital modem.
- Sync (1) indicates a non-ISDN synchronous connection, such as a Switched-56K connection.
- ISDN-Sync (2) indicates a synchronous ISDN connection.
- ISDN-Async-V120 (3) indicates an ISDN connection using V.120 asynchronous rate adaption.
- ISDN-Async-V110 (4) indicates an ISDN connection using V.110 asynchronous rate adaption.
- Virtual (5) indicates a connection to the TAOS unit using a transport protocol instead of a physical port.
- PIAFS (6) indicates a connection using the Personal Internet Access Forum Standard (PIAFS), a protocol that handles connection negotiation, data transfer, and error correction for the Personal Handyphone System (PHS).

Example: The following user profile specifies that the client is restricted to a synchronous ISDN connection:

```
Tom User-Password="mypw", Service-Type=Framed-User,
NAS-Port-Type=ISDN-Sync
    Framed-Protocol=PPP,
    Framed-IP-Address=200.250.55.9,
    Framed-IP-Netmask=255.255.255.248,
    Ascend-Link-Compression=Link-Comp-Stac-Draft-9,
    Ascend-Route-IP=Route-IP-Yes,
    Ascend-Metric=2
```

See Also: “NAS-Port (5)” on page 4-157.

Reply-Message (18)

Description: Carries message text from the RADIUS server to a RADIUS client (such as the TAOS unit). In a pseudo-user profile that configures message text and a list of IP hosts, the Reply-Message attribute specifies text that appears to the terminal-server operator at the menu-driven interface. In addition, if the RADIUS server determines that the TAOS unit should terminate the session, it sends an Access-Terminate-Session packet containing the Reply-Message attribute.

Usage: Specify a text string of up to 80 characters. The default value is null. You can specify up to 16 Reply-Message attributes in a pseudo-user profile.

Example: To set up message text for a TAOS unit named Cal, you could configure a pseudo-user profile as follows:

```
banner-Cal User-Password="ascend", Service-Type=Outbound-User
    Reply-Message="Up to 16 lines of up to 80 characters each",
    Reply-Message="will be accepted. ",
    Reply-Message="Additional lines will be ignored.",
    Reply-Message="",
    Ascend-Host-Info="1.2.3.4 Berkeley",
    Ascend-Host-Info="1.2.3.5 Alameda",
    Ascend-Host-Info="1.2.36 San Francisco"
```

Dependencies: Consider the following:

- An Access-Terminate-Session packet is a RADIUS packet identified by the code number 31. Only RADIUS daemons you customize to support this packet code can send an Access-Terminate-Session packet.
- If you do not specify a Reply-Message attribute in a user profile that authenticates callers, and the RADIUS server sends an Access-Accept packet, no message appears.
- If the RADIUS server sends an Access-Reject packet and you do not specify a Reply-Message attribute in a customized RADIUS daemon, the following message appears:

  ```
  ** Bad Password
  ```

- If the RADIUS server sends an Access-Terminate-Session packet and you do not specify a Reply-Message attribute in a customized RADIUS daemon, the TAOS unit displays the following message to the terminal-server user:

  ```
  ** Session Terminated
  ```

“Ascend-Host-Info (252)” on page 4-90.

Service-Type (6)

Description: Specifies the type of services the link can use.

Usage: Specify one of the following values:

- Login-User (1) specifies that the caller can use an asynchronous connection to log into the terminal server. The caller can start Telnet, Rlogin, or raw TCP sessions. The TAOS unit rejects incoming framed calls.
- Framed-User (2) specifies that incoming calls must use a framed protocol. If they do not, the TAOS unit rejects them.

- Callback-Login-User (3) specifies that the unit must call back the calling device before establishing an asynchronous link that enables the device to log into the terminal server.
- Callback-Framed-User (4) specifies that the unit must call back the calling device and establish a framed connection.
- Outbound-User (5) specifies that the TAOS unit can use the profile only for outgoing calls.

By default, the TAOS unit does not limit the services the link can access.

Example: To specify that a dial-in user can use only framed protocols, you could configure a user profile as follows:

```
Unit1 User-Password="mypw", Service-Type=Framed-User
       Framed-Protocol=PPP,
       Framed-IP-Address=10.0.200.225,
       Framed-IP-Netmask=255.255.255.0,
       Ascend-Metric=2,
       Framed-Routing=None,
       Framed-Route="10.0.220.0 10.0.200.225 1"
```

Dependencies: When you specify the Login-User or Callback-Login-User setting, the caller must have an asynchronous means of reaching the TAOS unit. The TAOS unit must have digital modems, or the call must be V.120 encapsulated.

See Also: The Service-Type attribute can appear in both an Access-Request and an Access-Accept packet.

Session-Timeout (27)

Description: Specifies the maximum number of seconds of service to be provided to the user before termination of the session or prompt.

Usage: Specify a number from 0 to 4,294,967,295. The default value is 0 (zero), which specifies that the TAOS unit does not enforce a time limit.

Example: The following user profile specifies that the user has a maximum limit of one hour of service:

```
smith User-Password="xyzzy"
   Service-Type=Framed-User,
   Framed-Protocol=PPP,
   Framed-IP-Address=10.0.200.225,
   Framed-IP-Netmask=255.255.255.0,
   Session-Timeout=3600
```

See Also: “Ascend-MPP-Idle-Percent (254)” on page 4-105 and “Ascend-Preempt-Limit (245)” on page 4-114.

State (24)

Description: A value sent by the RADIUS server to the TAOS unit in an Access-Challenge or Access-Accept packet. The TAOS unit can also send the State value to the server in an Access-Request packet.

Usage: The State attribute does not appear in a user profile.

Example: `State="cookie12345"`

See Also: "CHAP-Password (3)" on page 4-145.

Tunnel-Client-Auth-ID (90)

Description: Specifies the name of the Layer 2 Forwarding (L2F) tunnel initiator. The name is sent to the tunnel endpoint during tunnel authentication.

Usage: Specify a text string.

Example: The following user profile specifies a tunnel to a home gateway (1.1.1.1) and Calling-Line ID (CLID) authentication:

```
5551000 User-Password="Ascend-CLID", Service-Type=Outbound-User
    Tunnel-Client-ID-Auth="SanFran",
    Tunnel-Type=L2F,
    Tunnel-Medium-Type=IP,
    Tunnel-Server-Endpoint="1.1.1.1"
    Tunnel-Password="shared_secret"
```

Dependencies: Consider the following:

- The value of Tunnel-Client-Auth-ID overrides any L2F system name configured locally.
- Tunnel-Client-Auth-ID supports tagging.

See Also: "Tunnel-Medium-Type (65)" on page 4-162,
"Tunnel-Password (69)" on page 4-162,
"Tunnel-Server-Endpoint (67)" on page 4-165, and
"Tunnel-Type (64)" on page 4-166.

Tunnel-Client-Endpoint (66)

Description: Specifies a string assigned by RADIUS that specifies the name for the unit placing the call. This value is used by RADIUS accounting for tracking the session.

Usage: Tunnel-Client-Endpoint does not appear in a user profile.

Example: `Tunnel-Client-Endpoint="Dallas"`

Dependencies: Consider the following:

- DNIS or CLID authentication must be enabled.
- The TAOS unit must have RADIUS user entries that specify DNIS or CLID.

See Also: "Called-Station-Id (30)" on page 4-144.

Tunnel-ID (68)

Description: Specifies a string assigned by RADIUS to each session using CLID or DNIS tunneling. This value is used by RADIUS accounting for tracking the session.

Usage: Tunnel-ID does not appear in a user profile.

Example: `Tunnel-ID="1234567"`

Dependencies: Consider the following:

- DNIS or CLID must be enabled
- The TAOS unit must have RADIUS user entries that specify DNIS or CLID.

See Also: "Called-Station-Id (30)" on page 4-144.

Tunnel-Medium-Type (65)

Description: Specifies the media to be used for the tunnel.

Usage: Specify one of the following values:

- IP (1) specifies an Internet Protocol (IP) link.
- X25 (2) specifies an X.25 link.
- ATM (3) specifies an Asynchronous Transfer Mode (ATM) link.

Example: The following profile specifies that the unit opens an tunnel to an L2TP Network Server (LNS) at IP address 1.1.1.1 after verifying the caller ID:

```
5551000 User-Password="Ascend-CLID", Service-Type=Outbound-User
   Tunnel-Type=L2TP,
   Tunnel-Medium-Type=IP,
   Tunnel-Server-Endpoint="1.1.1.1"
```

Dependencies: Consider the following:

- DNIS or CLID must be enabled.
- The TAOS unit must have RADIUS user entries that specify DNIS or CLID.
- The Tunnel-Medium-Type attribute supports tagging.

See Also: "Tunnel-Server-Endpoint (67)" on page 4-165 and "Tunnel-Type (64)" on page 4-166.

Tunnel-Password (69)

Description: Specifies the password that the Foreign Agent sends to the Home Agent during Ascend Tunnel Management Protocol (ATMP) operation, or that the TAOS unit uses for authenticating Layer-2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels.

Usage: Specify a text string of up to 20 characters.

Example: The following user profile specifies the password that the ATMP Foreign Agent sends to the Home Agent:

```
mobile-client User-Password="my-password",
   Service-Type=Framed-User
   Tunnel-Type=ATMP,
   Tunnel-Server-Endpoint="3.3.3.3:8877",
   Tunnel-Password="tunnel-password"
```

Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3:

```
joe User-Password="murphy"
    Tunnel-Type=L2TP : 1,
    Tunnel-Server-Endpoint="1.1.1.1" : 1,
    Tunnel-Password="loloaqic" : 1,
    Tunnel-Type=L2TP : 3,
    Tunnel-Server-Endpoint="3.3.3.3" : 3,
    Tunnel-Password="i82qb4ip" : 3,
    Tunnel-Type=L2F : 2,
    Tunnel-Server-Endpoint="2.2.2.2" : 2
    Tunnel-Password="itsAsecret" : 2
```

This profile specifies that the the TAOS unit should attempt first to establish an L2TP tunnel to the LNS at 1.1.1.1. If that attempt fails, the system should attempt to bring up an L2F tunnel to a server at 2.2.2.2. If that attempt also fails, the system should try an L2TP tunnel to 3.3.3.3.

Dependencies: Consider the following:

- Under ATMP operation, all Mobile Clients accessing a single Home Agent must specify the same password.
- If you specify tagging for L2TP and L2F tunnels, all specified attribute sets are used. For ATMP, only the two sets with the highest priority are used. Priority is defined by the Tunnel-Preference value or by tag order.

If you are using RADIUS to authenticate L2F tunnels with distinct passwords, make sure of the following:

- The client's RADIUS user profile contains a Tunnel-Password attribute with the password that the TAOS uses to authenticate the tunnel to the home gateway.
- The home gateway has a RADIUS user profile. Because this is not a user profile for interactive access, Lucent recommends that the Service-Type be set to Outbound.

The following examples show a client's RADIUS profile and a home gateway's RADIUS profile that use for distinct secrets for tunnel authentication:

```
dialup-client User-Password="client-pw"
    Tunnel-Type=L2F,
    Tunnel-Server-Endpoint="1.1.1.1",
    Tunnel-Password="nas-secret"

hg-name User-Password="hg-secret", Service-Type=Outbound
    Reply-Message=""
```

See Also: "Tunnel-Server-Endpoint (67)" on page 4-165.

Tunnel-Preference (83)

Description: Specifies the numeric preference value for an attribute set.

Usage: .Specify a value from 255255255 (the lowest priority) to 000000 (the highest priority).

Example: In the following example, the user profile specifies that the TAOS unit first attempts to establish an L2F tunnel with an endpoint named `l2f-hgw`, then attempts to establish an L2TP tunnel with an LNS named `l2tp-lns`, and finally attempts to establish an L2TP tunnel with the endpoint at the IP address 200.168.121.1:

```
joebloggs User-Password="murphy"
   Tunnel-Type=L2TP:1,
   Tunnel-Server-Endpoint=l2tp-lns.lucent.com:1,
   Tunnel-Password=loloaqic:1,
   Tunnel-Type=L2TP:3,
   Tunnel-Server-Endpoint=200.168.121.1:3,
   Tunnel-Password=i82qb4ip:3,
   Tunnel-Type=L2F:2,
   Tunnel-Server-Endpoint=l2f-hgw.lucent.com:2
   Tunnel-Password=itsAsecret:2,
   Tunnel-Preference=200:1,
   Tunnel-Preference=100:2
```

Dependencies: Consider the following:

- If more than one set of tunneling attributes is returned by the RADIUS server to the TAOS unit, the Tunnel-Preference attribute can be included in a set to indicate its relative preference, with the lowest preference value designating the most preferred set.
- If no Tunnel-Preference is included in any of the attribute sets, the sets will be processed in the order of their respective tag numbers.
- If some but not all attribute sets contain a Tunnel-Preference value, the attribute sets without a Tunnel-Preference are designated as the least preferred sets.
- Attribute sets with identical preferences are processed in random order.
- The following RADIUS attributes support tagging: Ascend-Tunnel-VRouter-Name, Tunnel-Medium-Type, Tunnel-Password, Tunnel-Preference, Tunnel-Server-Endpoint, and Tunnel-Type.
- For L2TP and L2F, all specified attribute sets are used.
- For PPTP, only the attribute set with the highest priority is used. Priority is defined by the Tunnel-Preference value or by tag order.
- For ATMP, only the two sets with the highest priority are used. From the second attribute set, only the Tunnel-Server-Endpoint value is used. Other values can be omitted. Priority is defined by the Tunnel-Preference value or by tag order.

See Also: "Ascend-Tunnel-VRouter-Name (31)" on page 4-140,
"Tunnel-Medium-Type (65)" on page 4-162,
"Tunnel-Password (69)" on page 4-162,
"Tunnel-Server-Endpoint (67)" on page 4-165, and
"Tunnel-Type (64)" on page 4-166.

Tunnel-Private-Group-ID (81)

Description: Specifies the name of the Connection profile that defines the link on which the ATMP Home Agent transmits packets it receives from the Mobile Client.

Usage: Specify the name of the Connection profile.

Example: In the following user profile, the specified Connection profile is called `MyHomeNet`:

```
UL3 User-Password="example"
   Tunnel-Type=ATMP :1,
   Tunnel-Server-Endpoint=HA-a.example.com :1,
   Tunnel-Server-Endpoint=HA-b.example.com :2,
```

```
Tunnel-Password=HApassword :1,
Tunnel-Private-Group-ID=MyHomeNet :1
```

Dependencies: Tunnel-Private-Group-ID applies only if the Home Agent is in gateway mode. For an alternative setting, use Ascend-Home-Network-Name.

Location: "Ascend-Home-Network-Name (185)" on page 4-89.

Tunnel-Server-Endpoint (67)

Description: Specifies the IP address or hostname of the Ascend Tunnel Management Protocol (ATMP) primary Home Agent, L2TP Network Server (LNS) endpoint, PPTP Network Server (PNS) endpoint, L2F home gateway endpoint, or the destination that will decapsulate IP packets under IP-in-IP encapsulation.

Usage: Make your specification in the following format:

`Tunnel-Server-Endpoint="`*`hostname`* `|` *`ip_address`* `[:`*`udp_port`*`]"`

Table 4-23 lists each element of the syntax.

Table 4-23. Tunnel-Server-Endpoint syntax

Syntax element	Specifies
hostname	Symbolic hostname.
ip_address	IP address in dotted decimal notation. Specify an IP address if a DNS server is not set up. You can specify a host name or an IP address, but not both. The IP address should be the system address, not the IP address of the interface on which the unit receives tunneled data.
udp_port	UDP port on which the Foreign Agent communicates with the Home Agent. The default value is 5150.
`:` (colon)	Separator between the hostname (or IP address) and the UDP port.

Example: To specify the Home Agent `taos.home.com` at IP address 10.0.0.1, and indicate that the Foreign Agent should use UDP port 6001, enter one of the following lines in a RADIUS user profile:

```
Tunnel-Server-Endpoint="taos.home.com:6001"
Tunnel-Server-Endpoint="10.0.0.1:6001"
```

Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3:

```
joe User-Password="murphy"
    Tunnel-Type=L2TP : 1,
    Tunnel-Server-Endpoint="1.1.1.1" : 1,
    Tunnel-Password="loloaqic" : 1,
    Tunnel-Type=L2TP : 3,
    Tunnel-Server-Endpoint="3.3.3.3" : 3,
    Tunnel-Password="i82qb4ip" : 3,
    Tunnel-Type=L2F : 2,
```

```
Tunnel-Server-Endpoint="2.2.2.2" : 2
Tunnel-Password="itsAsecret" : 2
```

This profile specifies that the the TAOS unit should attempt first to establish an L2TP tunnel to the LNS at 1.1.1.1. If that attempt fails, the system should attempt to bring up an L2F tunnel to a server at 2.2.2.2. If that attempt also fails, the system should try an L2TP tunnel to 3.3.3.3.

Dependencies: Consider the following:

- If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Tunnel-Server-Endpoint attribute, you need not specify a value for *udp_port*.
- If you specify a value for the *udp_port* argument of Tunnel-Server-Endpoint, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.
- Use Tunnel-Server-Endpoint instead of the Ascend-Primary-Home-Agent attribute.
- To specify a secondary Home Agent for use if the primary Home Agent is unavailable, enter a value for the Ascend-Secondary-Home-Agent attribute.

If you specify tagging, keep the following information in mind:

- For L2TP and L2F, all specified attribute sets are used.
- For PPTP, only the attribute set with the highest priority is used. Priority is defined by the Tunnel-Preference value or by tag order.
- For ATMP, only the two sets with the highest priority are used. From the second attribute set, only the Tunnel-Server-Endpoint value is used. Other values can be omitted. Priority is defined by the Tunnel-Preference value or by tag order.

See Also: "Ascend-Home-Agent-UDP-Port (186)" on page 4-89,
"Ascend-Home-Network-Name (185)" on page 4-89,
"Ascend-Secondary-Home-Agent (130)" on page 4-128,
"Tunnel-Medium-Type (65)" on page 4-162,
"Tunnel-Server-Endpoint (67)" on page 4-165, and
"Tunnel-Type (64)" on page 4-166.

Tunnel-Type (64)

Description: Specifies the tunneling protocol to use.

Usage: Specify one of the following values:

- PPTP (1) specifies Point-to-Point Tunneling Protocol.
- L2F (2) specifies Layer 2 Forwarding.
- L2TP (3) specifies Layer 2 Tunneling Protocol.
- ATMP (4) specifies Ascend Tunnel Management Protocol.
- VTP (5) specifies Virtual Tunneling Protocol.
- IP-in-IP (7) specifies that IP packets are encapsulated in IP.

Example: The following the following user profile specifies CLID authentication for an L2TP tunnel to an L2TP Network Server (LNS) at 200.10.10.1:

```
5551000 User-Password="Ascend-CLID", Service-Type=Outbound-User
   Tunnel-Type=L2TP,
   Tunnel-Medium-Type=IP
   Tunnel-Server-Endpoint=200.10.10.1
```

Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3:

```
joe User-Password="murphy"
    Tunnel-Type=L2TP : 1,
    Tunnel-Server-Endpoint="1.1.1.1" : 1,
    Tunnel-Password="loloaqic" : 1,
    Tunnel-Type=L2TP : 3,
    Tunnel-Server-Endpoint="3.3.3.3" : 3,
    Tunnel-Password="i82qb4ip" : 3,
    Tunnel-Type=L2F : 2,
    Tunnel-Server-Endpoint="2.2.2.2" : 2
    Tunnel-Password="itsAsecret" : 2
```

This profile specifies that the the TAOS unit should attempt first to establish an L2TP tunnel to the LNS at 1.1.1.1. If that attempt fails, the system should attempt to bring up an L2F tunnel to a server at 2.2.2.2. If that attempt also fails, the system should try an L2TP tunnel to 3.3.3.3.

Dependencies: Only L2F and L2TP currently operate with full tunnel attribute and tag support. For L2TP and L2F, all specified attribute sets are used.

See Also: "Tunnel-Medium-Type (65)" on page 4-162 and "Tunnel-Server-Endpoint (67)" on page 4-165.

User-Name (1)

Description: Specifies one of the following:

- The name of the calling device or dial-in user
- The keyword Default
- The incoming phone number (for CLID authentication)
- The called-party number (for called-number authentication)
- The name of a pseudo-user profile

Usage: Specify an alphanumeric string of up to 252 characters. The default value is null. The user name must be the first word in a user profile. You need not specify the name of the attribute.

Example: Suppose you enter the following first line of a user profile for a user named Emma:

```
Emma User-Password="pwd", Ascend-PW-Expiration="Dec 31 1999"
```

The RADIUS server tests the user's name and password against the values the user provides when making a request for access. If the RADIUS server does not find a match, it denies the request for access.

To use CLID authentication with the incoming phone number as the User-Name, you could configure a user profile as follows:

```
5551212  User-Password="Ascend-CLID"
         Ascend-Require-Auth=Not-Require-Auth,
```

```
Service-Type=Framed-User,
Framed-Protocol=PPP,
Framed-IP-Address=255.255.255.254,
Framed-IP-Netmask=255.255.255.255,
Ascend-Route-IP=Route-IP-Yes
```

Finally, the following example shows how you would enter User-Name in a pseudo-user profile for a static route:

```
route-1 User-Password="ascend", Service-Type=Outbound-User
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out"
```

Dependencies: Consider the following:

- If the system performs only first-tier Dialed Number Information Service (DNIS) authentication, and the RADIUS user profile specifies a value for User-Name, the RADIUS server returns the value of the User-Name attribute in its DNIS Auth reply. The User-Name value then appears in SNMP serviceChanged events and the session table, in Syslog messages, and in RADIUS Start/Stop records.
- When a dial-in client uses Rlogin, the TAOS unit can use the value of User-Name in the user's RADIUS profile as the UNIX login name. If the user's profile does not specify a User-Name value, the user is still required to enter the UNIX username on the Rlogin command line, but if the user's profile does specify a User-Name value, all subsequent Rlogins use that name as the default name for Rlogin commands.

See Also: "User-Password (2)" on page 4-168.

User-Password (2)

Description: Specifies the password of the calling device or dial-in user.

Usage: Specify an alphanumeric string of up to 252 characters. The default value is null. The User-Password attribute must appear on the first line of the user profile.

Example: Suppose you enter the following first line of a user profile for a user named Emma:

```
Emma User-Password="pwd", Ascend-PW-Expiration="Dec 31 1999"
```

The RADIUS server tests the user's name and password against the values the user provides when making a request for access. If the RADIUS server does not find a match, it denies the request for access.

See Also: "User-Name (1)" on page 4-167.

Vendor-Specific (26)

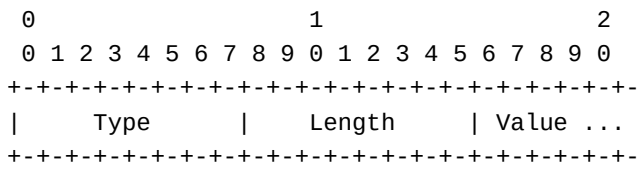
Description: Encapsulates attributes introduced by vendors. The purpose of the Vendor-Specific attribute is to enable companies to extend RADIUS operations without leading to possible attribute collisions (two attributes with the same type number but different meanings).

RFC 2138, *Remote Authentication Dial In User Service (RADIUS),* defines the Vendor-Specific attribute, specifying methods of handling vendor extensions and of encrypting and decrypting the User-Password. The RFC-defined methods differ from the way Ascend implemented these functions in the past. In the past, Ascend extended RADIUS

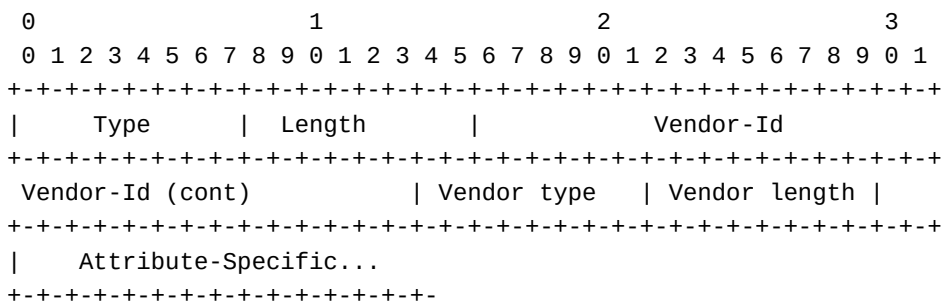
operations by adding Ascend vendor attributes, such as Ascend-Xmit-Rate, and used its own algorithm for User-Password encryption.

Now, you can configure the TAOS unit with support for the Vendor-Specific Attribute (VSA) and the RFC-defined User-Password encryption algorithm. Lucent maintains backward compatibility by making VSA compatibility mode configurable. However, attributes of Type 91 or smaller are available only in VSA compatibility mode. Attributes of Type 92 or higher are available in both VSA compatibility mode and the default mode, which is compatible with older Ascend implementations.

The format of Lucent vendor attributes in a request or response is new. The older Ascend format for all attributes is as follows:



The format of the VSA (as defined in RFC 2138) is as follows:


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Vendor-Id
Vendor-Id (cont)
Vendor type
Vendor length
Attribute-Specific...

The Type of the VSA is 26. The Length is 8 or greater. Lucent's Vendor-Id is 529.

The Vendor Type, Vendor Length, and Attribute-Specific Value are the same as the Type, Length, and Value of the unencapsulated Ascend attribute. For example, the Type of the Ascend-Xmit-Rate attribute is 255. Because it is an integer, it has a Length of 6. The Value is the transmit rate of the connection. So, the fields of the VSA will specify the following values:

- Type=26
- Length=12
- Vendor-Id=529
- Vendor Type=255
- Vendor Length=6
- Attribute-Specific Value=*transmit-rate*

Note: Some vendors have interpreted RFC 2138 to allow packing more than one vendor attribute in a single VSA. Lucent does not support this use. The TAOS unit sends a single vendor attribute per VSA. If it receives a VSA that contains more than one vendor attribute, it recognizes the first vendor attribute and ignores the rest.

Free-RADIUS attributes and their RFC equivalents

Free-RADIUS attributes are not supported after release 7.0.0. They are not RFC compliant, nor are they compatible with VSA attributes.

Some standard RFC 2138 attributes have free-RADIUS equivalents that use different names. Table 4-24 contains a list of free-RADIUS attributes and their RFC 2138 equivalents.

Table 4-24. Free-RADIUS attributes and their RFC 2138 equivalents

Free-RADIUS attribute	RFC 2138 equivalent
Caller-Id (31)	Calling-Station-Id (31)
Challenge-Response (3)	CHAP-Password (3)
Client-Port-DNIS (30)	Called-Station-Id (30)
Framed-Address (8)	Framed-IP-Address (8)
Framed-Netmask (9)	Framed-IP-Netmask (9)
Login-Host (14)	Login-IP-Host (14)
NAS-Identifier (4)	NAS-IP-Address (4)
Password (2)	User-Password (2)
User-Service (6)	Service-Type (6)

As indicated by Table 4-24, the free-RADIUS User-Service attribute has been replaced by the RFC-compliant Service-Type attribute. Table 4-25 lists the User-Service settings and their Service-Type equivalents.

Table 4-25. User-Service settings and their Service-Type equivalents

User-Service	Service-Type setting
Login-User (1)	Login-User (1)
Framed-User (2)	Framed-User (2)
Dialback-Login-User (3)	Callback-Login-User (3)
Dialback-Framed-User (4)	Callback-Framed-User (4)
Dialout-Framed-User (5)	Outbound-User (5)

RFC-standard attributes not supported by TAOS

Table 4-26 lists the RFC-standard attributes that are not supported by TAOS, and TAOS equivalents (where applicable).

Table 4-26. RFC-standard attributes not supported by TAOS

RFC-standard attribute	TAOS equivalent
Callback-ID (20)	User-Name (1) provides identical functionality.
Callback-Number (19)	Ascend-Dial-Number (227) provides identical functionality.
NAS-Identifier (32)	NAS-IP-Address (4) provides identical functionality.
Proxy-State (33)	N/A
Framed-AppleTalk-Link (37)	Ascend-Appletalk-Route (116) provides similar (but not identical) functionality.
Framed-AppleTalk-Network (38)	Ascend-Appletalk-Route (116) provides similar (but not identical) functionality.
Framed-AppleTalk-Zone (39)	Ascend-Appletalk-Route (116) provides similar (but not identical) functionality.
Login-LAT-Group (36)	N/A
Login-LAT-Node (35)	N/A
Login-LAT-Port (63)	N/A
Login-LAT-Service (34)	N/A
Port-Limit (62)	Ascend-Shared-Profile-Enable (128) and Ascend-Maximum-Channels (235) provide similar (but not identical) functionality.
CHAP-Challenge (60)	N/A

Unused attributes

The following attributes are currently unused:

- Ascend-CBCP-Delay (114)
- Ascend-FR-LinkUp (157)
- Tunnel-Assignment-ID (81)
- Tunnel-Server-Auth-ID (91)

Outdated attributes

Table 4-27 lists old attributes that have been replaced by new ones.

Table 4-27. Outdated RADIUS attributes

Old attribute	Replaced by
Ascend-Encaps	Framed-Protocol
Ascend-IF-Addr	Ascend-PPP-Address
Ascend-IP-Address	Framed-IP-Address
Ascend-IPX-Network	Framed-IPX-Network
Ascend-MRU	Framed-MTU
Ascend-Netmask	Framed-IP-Netmask
Ascend-RIP	Framed-Routing
Ascend-Station	User-Name
Ascend-Terminal-Banner	Reply-Message
Ascend-VJ-Compression	Framed-Compression

Contents of RADIUS Packets

A

Access-Request (1) A-2

Access-Accept (2) A-3

Access-Reject (3) A-8

Access-Password-Request (7) A-8

Access-Password-Ack (8) A-9

Access-Password-Reject (9) A-9

Access-Challenge (11) A-9

Access-Password-Expired (32) A-9

Ascend-Access-Event-Request (33) A-9

Ascend-Access-Event-Response (34) A-9

Ascend-Disconnect-Request (40) A-10

Ascend-Disconnect-Ack (41) A-10

Ascend-Disconnect-Nak (42) A-10

Ascend-Change-Filters-Request (43) A-10

Ascend-Change-Filters-Ack (44) A-10

Ascend-Change-Filters-Nak (45) A-10

This appendix lists the packets and RADIUS attributes associated with authentication, connection setup, and user sessions. For information about attributes associated with accounting, see Chapter 3, “Understanding RADIUS Accounting.”.

Access-Request (1)

By default, when it receives an incoming call, the TAOS unit first checks its local Connection profiles. If it doesn't find a Connection profile for the call, and you have configured the TAOS unit to communicate with RADIUS, the TAOS unit sends an Access-Request packet to the RADIUS server. The Access-Request packet includes the caller's name and password, and might also include the other attributes listed here:

- Ascend-Calling-Id-Numbering-Plan (67)
- Ascend-Calling-Id-Presentation (68)
- Ascend-Calling-Id-Screening (69)
- Ascend-Calling-Id-Type-Of-Number (66)
- Ascend-Calling-Subaddress (107)
- Ascend-Data-Rate (197)—Only when the connection is *not* authenticated by means of Calling-Line ID (CLID) or Dialed Number Information Service (DNIS).
- Ascend-Send-Passwd (232)
- Ascend-Send-Secret (214)
- Ascend-Xmit-Rate (255)—Only when the connection is *not* authenticated by means of Calling-Line ID (CLID) or Dialed Number Information Service (DNIS).
- Called-Station-Id (30)
- Calling-Station-Id (31)
- CHAP-Password (3)
- Class (25)
- Framed-Protocol (7)
- MS-CHAP-Challenge
- MS-CHAP-Response
- NAS-IP-Address (4)
- NAS-Port (5)
- NAS-Port-Type (61)
- Service-Type (6)
- State (24)
- User-Name (1)
- User-Password (2)

Access-Accept (2)

If the attribute values the TAOS unit submits to RADIUS match the attribute values in the user profile, the RADIUS server authenticates the call and returns an Access-Accept packet containing a list of attributes characterizing that user. The following Access-Accept attributes are defined in RFC 2138:

- Called-Station-Id (30)
- Calling-Station-Id (31)
- Change-Password (17)
- Class (25)
- Filter-ID (11)
- Framed-Compression (13)
- Framed-IP-Address (8)
- Framed-IP-Netmask (9)
- Framed-IPX-Network (23)
- Framed-MTU (12)
- Framed-Protocol (7)
- Framed-Route (22)
- Framed-Routing (10)
- Idle-Timeout (28)
- Login-IP-Host (14)
- Login-Service (15)
- Login-TCP-Port (16)
- Service-Type (6)
- Session-Timeout (27)
- State (24)
- Tunnel-Client-Auth-ID (90)
- Tunnel-Medium-Type (65)
- Tunnel-Password (69)
- Tunnel-Preference (83)
- Tunnel-Private-Group-ID (81)
- Tunnel-Server-Endpoint (67)
- Tunnel-Type (64)
- Vendor-Specific (26)

The following attributes are Lucent extensions to the RADIUS attributes:

- Ascend-Add-Seconds (240)
- Ascend-Appletalk-Peer-Mode (117)
- Ascend-Appletalk-Route (116)
- Ascend-ARA-PW (181)
- Ascend-Assign-IP-Client (144)

- Ascend-Assign-IP-Global-Pool (146)
- Ascend-Assign-IP-Pool (218)
- Ascend-Assign-IP-Server (145)
- Ascend-ATM-Connect-Group (63)
- Ascend-ATM-Connect-Vci (62)
- Ascend-ATM-Connect-Vpi (61)
- Ascend-ATM-Direct (76)
- Ascend-ATM-Direct-Profile (77)
- Ascend-ATM-Fault-Management (14)
- Ascend-ATM-Group (64)
- Ascend-ATM-Loopback-Cell-Loss (15)
- Ascend-ATM-Vci (95)
- Ascend-ATM-Vpi (94)
- Ascend-Authen-Alias (203)
- Ascend-Auth-Type (81)
- Ascend-Backup (176)
- Ascend-BACP-Enable (133)
- Ascend-Base-Channel-Count (172)
- Ascend-Bi-Directional-Auth (46)
- Ascend-Billing-Number (249)
- Ascend-BIR-Bridge-Group (72)
- Ascend-BIR-Enable (70)
- Ascend-BIR-Proxy (71)
- Ascend-Bridge (230)
- Ascend-Bridge-Address (168)
- Ascend-Bridge-Non-PPPoE (75)
- Ascend-Cache-Time (57)
- Ascend-Cache-Refresh (56)
- Ascend-Call-Attempt-Limit (123
- Ascend-Callback (246)
- Ascend-Callback-Delay (108)
- Ascend-Call-Block-Duration (124)
- Ascend-Call-By-Call (250)
- Ascend-Call-Filter (243)
- Ascend-Call-Type (177)
- Ascend-CBCP-Enable (112)
- Ascend-CBCP-Mode (113)
- Ascend-CBCP-Trunk-Group (115)
- Ascend-Ckt-Type (16)

- Ascend-Client-Assign-DNS (137)
- Ascend-Client-Assign-WINS (80)
- Ascend-Client-Primary-DNS (135)
- Ascend-Client-Primary-WINS (78)
- Ascend-Client-Secondary-DNS (136)
- Ascend-Client-Secondary-WINS (79)
- Ascend-Data-Filter (242)
- Ascend-Data-Svc (247)
- Ascend-DBA-Monitor (171)
- Ascend-Dec-Channel-Count (237)
- Ascend-DHCP-Maximum-Leases (134)
- Ascend-DHCP-Pool-Number (148)
- Ascend-DHCP-Reply (147)
- Ascend-Dial-Number (227)
- Ascend-Dialout-Allowed (131)
- Ascend-Dsl-CIR-Recv-Limit (100)
- Ascend-Dsl-CIR-Xmit-Limit (101)
- Ascend-DSL-Downstream-Limit (99)
- Ascend-Dsl-Rate-Type (92)
- Ascend-Dsl-Rate-Mode (97)
- Ascend-DSL-Upstream-Limit (98)
- Ascend-Egress-Enabled (58)
- Ascend-Endpoint-Disc (109)
- Ascend-Expect-Callback (149)
- Ascend-FCP-Parameter (119)
- Ascend-Filter (91)
- Ascend-Filter-Required (50)
- Ascend-First-Dest (189)
- Ascend-Force-56 (248)
- Ascend-FR-08-Mode (10)
- Ascend-FR-Circuit-Name (156)
- Ascend-FR-DCE-N392 (162)
- Ascend-FR-DCE-N393 (164)
- Ascend-FR-Direct (219)
- Ascend-FR-Direct-DLCI (221)
- Ascend-FR-Direct-Profile (220)
- Ascend-FR-DLCI (179)
- Ascend-FR-DTE-N392 (163)
- Ascend-FR-DTE-N393 (165)

- Ascend-FR-Link-Mgt (160)
- Ascend-FR-Link-Status-DLCI (106)
- Ascend-FR-N391 (161)
- Ascend-FR-Nailed-Grp (158)
- Ascend-FR-Profile-Name (180)
- Ascend-FR-SVC-Addr (12)
- Ascend-FR-T391 (166)
- Ascend-FR-T392 (167)
- Ascend-FR-Type (159)
- Ascend-FT1-Caller (175)
- Ascend-Group (178)
- Ascend-Handle-IPX (222)
- Ascend-History-Weigh-Type (239)
- Ascend-Home-Agent-UDP-Port (186)
- Ascend-Home-Network-Name (185)
- Ascend-Host-Info (252)
- Ascend-IF-Netmask (153)
- Ascend-Inc-Channel-Count (236)
- Ascend-IP-Direct (209)
- Ascend-IP-Pool-Chaining (85)
- Ascend-IP-Pool-Definition (217)
- Ascend-IPSEC-Profile (73)
- Ascend-IP-TOS (88)
- Ascend-IP-TOS-Apply-To (90)
- Ascend-IP-TOS-Precedence (89)
- Ascend-IPX-Alias (224)
- Ascend-IPX-Header-Compression (65)
- Ascend-IPX-Node-Addr (182)
- Ascend-IPX-Peer-Mode (216)
- Ascend-IPX-Route (174)
- Ascend-Link-Compression (233)
- Ascend-Maximum-Call-Duration (125)
- Ascend-Maximum-Channels (235)
- Ascend-Menu-Item (206)
- Ascend-Menu-Selector (205)
- Ascend-Metric (225)
- Ascend-Minimum-Channels (173)
- Ascend-MPP-Idle-Percent (254)
- Ascend-MTU (49)

- Ascend-Multicast-Client (155)
- Ascend-Multicast-GLeave-Delay (111)
- Ascend-Multicast-Rate-Limit (152)
- Ascend-Multilink-ID (187)
- Ascend-Netware-timeout (223)
- Ascend-Numbering-Plan-ID (105)
- Ascend-Num-In-Multilink (188)
- Ascend-Port-Redir-Portnum (83)
- Ascend-Port-Redir-Protocol (82)
- Ascend-Port-Redir-Server (84)
- Ascend-PPP-Address (253)
- Ascend-PPP-Async-Map (212)
- Ascend-PPPoE-Enable (74)
- Ascend-PPP-VJ-1172 (211)
- Ascend-PPP-VJ-Slot-Comp (210)
- Ascend-Preempt-Limit (245)
- Ascend-Pre-Input-Octets (190)
- Ascend-Pre-Input-Packets (192)
- Ascend-Pre-Output-Octets (191)
- Ascend-Pre-Output-Packets (193)
- Ascend-PRI-Number-Type (226)
- Ascend-Private-Route (104)
- Ascend-Private-Route-Required (55)
- Ascend-Private-Route-Table-ID (54)
- Ascend-PW-Expiration (21)
- Ascend-PW-Lifetime (208)
- Ascend-PW-Warntime (207)
- Ascend-QOS-Downstream (60)
- Ascend-QOS-Upstream (59)
- Ascend-Receive-Secret (215)
- Ascend-Recv-Name (45)
- Ascend-Remote-Addr (154)
- Ascend-Remote-FW (110)
- Ascend-Remove-Seconds (241)
- Ascend-Require-Auth (201)
- Ascend-Route-Appletalk (118)
- Ascend-Route-IP (228)
- Ascend-Route-IPX (229)
- Ascend-Route-Preference (126)

- Ascend-Secondary-Home-Agent (130)
- Ascend-Seconds-Of-History (238)
- Ascend-Send-Auth (231)
- Ascend-Send-Passwd (232)
- Ascend-Send-Secret (214)
- Ascend-Shared-Profile-Enable (128)
- Ascend-Source-Auth (103)
- Ascend-Source-IP-Check (96)
- Ascend-SVC-Enabled (17)
- Ascend-Target-Util (234)
- Ascend-Telnet-Profile (91)
- Ascend-Third-Prompt (213)
- Ascend-Token-Expiry (204)
- Ascend-Token-Idle (199)
- Ascend-Token-Immediate (200)
- Ascend-Traffic-Shaper (51)
- Ascend-Transit-Number (251)
- Ascend-Tunnel-VRouter-Name (31)
- Ascend-TS-Idle-Limit (169)
- Ascend-TS-Idle-Mode (170)
- Ascend-VRouter-Name (102)

Access-Reject (3)

If the attribute values submitted to RADIUS do not match the attribute values in the user profile, the RADIUS server does not authenticate the call. It returns an Access-Reject packet containing one or more of the following values:

- Login-TCP-Port (16)
- Reply-Message (18)

Access-Password-Request (7)

The following attributes appear in an Access-Password-Request packet:

- Change-Password (17)
- User-Name (1)
- User-Password (2)

Access-Password-Ack (8)

The Access-Password-Ack packet contains no attributes. The RADIUS server sends it to the TAOS unit to signal that a new password has been accepted.

Access-Password-Reject (9)

The Access-Password-Reject packet contains the Reply-Message (18) attribute.

Access-Challenge (11)

An Access-Challenge packet can contain the following attributes:

- MS-CHAP-Challenge
- Reply-Message (18)
- State (24)

Access-Password-Expired (32)

An Access-Password-Expired packet contains the Reply-Message (18).

Ascend-Access-Event-Request (33)

The TAOS unit can report the number of sessions by class to the RADIUS authentication server and to the RADIUS accounting server. The TAOS unit reports the number of sessions by sending an Ascend-Access-Event-Request (33) packet type at a user-defined interval. Following are the attributes in an Ascend-Access-Event-Request packet:

- NAS-IP-Address (4) (authentication and accounting requests)
- User-Password (2) (authentication requests only)
- Ascend-Event-Type (150) (authentication and accounting requests)
- Ascend-Number-Sessions (202) (authentication and accounting requests)

Ascend-Access-Event-Response (34)

Following are the attributes in an Ascend-Access-Event-Response packet:

- NAS-IP-Address (4) (authentication and accounting responses)
- Ascend-Event-Type (150) (authentication and accounting responses)
- Ascend-Number-Sessions (202) (authentication and accounting responses)

Ascend-Disconnect-Request (40)

Following are the attributes in an Ascend-Disconnect-Request packet:

- User-Name (1)
- Framed-IP-Address (8)
- Acct-Session-Id (44)
- Ascend-Session-Svr-Key (151)

Ascend-Disconnect-Ack (41)

If RADIUS found at least one session it could disconnect, the response code is 41 (Disconnect-Request-Ack). RADIUS does not return any attributes in the response.

Ascend-Disconnect-Nak (42)

If RADIUS did not find at least one session it could disconnect, the response code is 42 (Disconnect-Request-Nak). RADIUS does not return any attributes in the response.

Ascend-Change-Filters-Request (43)

In a Change-Filter-Request packet, the following attributes control filter changes:

- User-Name (1)
- Framed-IP-Address (8)
- Acct-Session-Id (44)
- Ascend-Data-Filter (242)
- Ascend-Call-Filter (243)
- Ascend-Session-Svr-Key (151)

Ascend-Change-Filters-Ack (44)

If RADIUS found at least one routing session whose filters it could change, the response code is 44 (Change-Filter-Request-Ack). RADIUS does not return any attributes in the response.

Ascend-Change-Filters-Nak (45)

If RADIUS did not find at least one routing session whose filters it could change, the response code is 45 (Change-Filter-Request-Nak).

Sample RADIUS Users File

B

This appendix contains an example of how you might set up a RADIUS users file. If you plan to use this example as a template, be sure to properly modify any site-specific settings before you use the file.

```
#  S A M P L E   R A D I U S   U S E R S   F I L E
#
#  This file contains security and configuration information
#  for each user. The first field is the user's name,
#  followed (on the same line) with the list of authentication
#  requirements for the user. These can include password, user name,
#  and an expiration date for the user's password. When an
#  authentication request is received from the unit, these values
#  are tested. A special user named "DEFAULT" can be created (and
#  should be placed at the end of the users file) to specify what to do
#  with users not contained in the users file. A special password of
#  "UNIX" can be specified to notify the authentication server to use
#  UNIX password (/etc/passwd) authentication for the user.
#
#  Line indented by means of the Tab character following the first
#  line indicate the configuration values to be passed back to
#  the unit to allow the initiation of a user session.
#  These can include things like the PPP configuration values.
#
#  Sample users file entries follow:

#  The following profile can only be used for PPP sessions.
#  It uses a local password.
#
testUser-Password = "test"
    Service-Type = Framed-User,
    Framed-Protocol = MPP,
    Ascend-Assign-IP-Pool = 1,
    Framed-Routing = None
```

```
#  The following profile uses the UNIX password file so that
#  the password does not have to be stored locally.
#
Unit2User-Password = "UNIX"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 10.0.2.1,
   Framed-IP-Netmask = 255.255.255.0

#  The following profile provides authentication by means of the
#  Enigma Logic SafeWord dynamic password library.
#
Unit3User-Password = "SAFEWORD"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 10.0.3.1,
   Framed-IP-Netmask = 255.255.255.0

#  The following profile provides authentication, by means of the
#  Enigma Logic SafeWord dynamic password library, with token caching
#  for 90 minutes.
#
Unit4User-Password = "SAFEWORD", Ascend-Token-Expiry = 90
   Ascend-Receive-Secret = "shared secret",
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 10.0.3.1,
   Framed-IP-Netmask = 255.255.255.0

#  The following profile provides authentication by means of the
#  Security Dynamics ACE dynamic password library, with token caching
#  for 540 minutes (9 hours) and an idle time of 80 minutes. "Idle"
#  means without a new call authentication, *not* without a call being
#  up. This example specifies that tokens should be cached all day and
#  allows a break as long as it doesn't exceed 80 minutes.
#
Unit5User-Password = "ACE", Ascend-Token-Expiry = 540,
Ascend-Token-Idle = 80
   Ascend-Receive-Secret = "shared secret",
   Service-Type = Framed-User,
```

```
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.0.3.1,
    Framed-IP-Netmask = 255.255.255.0

#   The following profile provides authentication by means of the
#   Security Dynamics ACE dynamic password library, with no challenge.
#   The dynamic password is entered in place of the usual "static"
#   password. The profile is useful only for modem dial-in calls.
#
Unit6User-Password = "ACE", Ascend-Token-Immediate = Tok-Imm-Yes
    Service-Type = Login-User,
    Login-Service = Telnet,
    Login-IP-Host = 10.0.4.1

#   The following profile provides authentication by means of the
#   Enigma Logic SafeWord dynamic password library, with no challenge.
#   The dynamic password is entered in place of the usual "static"
#   password. The profile is useful only for modem dial-in calls.
#
Unit7User-Password = "SAFEWORD", Ascend-Token-Immediate = Tok-Imm-Yes
    Service-Type = Login-User,
    Login-Service = Telnet,
    Login-IP-Host = 10.0.4.1

#
#
#   An ACE entry may be used to authenticate multiple users behind a
#   single remote router, such as a Pipeline unit. The following
#   entry uses the Pipeline unit's name, and password = ACE, as usual.
#   However, when the user enters the password, he or she specifies
#   <password><.><realname> instead of just <password>. In this case,
#   <realname> will be presented to the ACE server, rather than the
#   Pipeline unit's name. Token caching will still function normally.
#   All users will share the same profile, and all accounting will use
#   the Pipeline unit's name, not the real user name.
#
#   The following profile can only be used for PPP sessions. An
#   address will be assigned from address pool 1. A route to 10.0.0.1
#   is added with the user's address as the gateway.
```

```
#
UnitA User-Password = "pipeline"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-Routing = None,
    Ascend-Assign-IP-Pool = 1,
    Framed-Route = "10.0.0.1 0.0.0.0 1"

#   The following profile causes the unit to start an auto-Telnet
#   to 10.0.4.1 upon login.
#
userUser-Password = "xyzzy"
    Service-Type = Login-User,
    Login-Service = Telnet,
    Login-IP-Host = 10.0.4.1

#   The following profile causes the password to expire on 99/01/30.
#   If the password is changed remotely, the new password will have
#   a duration of 180 days.
#
useraUser-Password = "ageing", Ascend-PW-Expiration = "Jan 1 1999"
    Service-Type = Login-User,
    Login-Service = Telnet,
    Ascend-PW-Lifetime = 180

#   Use the following profile as a template for ARA user access.
#   NOTE: The password and Ascend-Send-Secret MUST be
#   identical
#
userxyz User-Password = "abcdef"
    Framed-Protocol = ARA,
    Ascend-Send-Secret = "abcdef"

#   The following profile causes the unit to start a raw TCP connection
#   to 10.0.5.1, port 23.
#
test1User-Password = "test1"
    Login-Service = TCP-Clear,
    Login-IP-Host = 10.0.5.1,
```

```
    Login-TCP-Port = 23

#   The following profile causes the unit to start a raw TCP connection
#   to 10.0.6.1, port 7.
#
test2User-Password = "test2"
    Login-Service = TCP-Clear,
    Login-IP-Host = 10.0.6.1,
    Login-TCP-Port = 7

#   The following profile causes the unit to start a Telnet connection
#   to 10.0.7.1, port 25.
#
test3User-Password = "test3"
    Login-Service = Telnet,
    Login-IP-Host = 10.0.7.1,
    Login-TCP-Port = 25

#   The following profile specifies a unit on a subnet dialing in
#   across a T1/PRI link, using a maximum of 23 channels.
#
maxUser-Password = "max"
    Framed-IP-Address = 10.0.8.1,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Metric = 1,
    Ascend-Maximum-Channels = 23,
    Ascend-Link-Compression = Link-Comp-None,
    Idle-Timeout = 30

#   The following profile specifies a Pipeline unit performing IPX
#   routing only.
#
ipxtest User-Password = "netware"
    Ascend-Route-IPX = Route-IPX-Yes,
    Ascend-Route-IP = Route-IP-No,
    Ascend-IPX-Peer-Mode = Peer-Mode-Router


#   P S E U D O-U S E R S
```

```
#
#  These 'users' exist to store information that the unit can query.
#  The profiles are not intended for real login users. The
#  password for pseudo-users is always "ascend". Each pseudo-user
#  profile includes a "Service-Type" attribute of Outbound-User
#  so that it cannot be used for user authentication.
#
#  Following are the pseudo-users you can specify:
#
#  banner:Storage of the terminal-server menu mode,
#         login banner, and table of host addresses
#         with descriptive text for the login menu.
#
#  pools-xxx:Definitions of address pools used by the
#         unit named xxx. The unit can support
#         several address pools. Two can be defined
#         in the unit. Those two can be overridden
#         and more defined from RADIUS.
#
#  route-n:A series of pseudo-users fetched by the
#         unit to initialize its routing table.
#         The unit queries route-1, then route-2,
#         then route-3, and so on, until it receives an
#         authentication reject from RADIUS. Each entry
#         should be limited to about 25 routes.
#         (25 routes @ 50 char/route = 1250 characters.
#         Add RADIUS overhead and each entry will still fit
#         into one Ethernet packet.)
#
#  outdial users:The static routes specified in the route-n entries
#         can contain a name. The name is used to look up
#         a RADIUS pseudo-user to obtain out-dial information.
#         At this time separate entries are required for
#         both in-dial and out-dial users.
#         It is recommended (but not required) that user
#         X have an out-dial entry named X-out. See the
#         examples below.

#  B A N N E R   P S E U D O - U S E R
```

```
#
bannerUser-Password = "ascend", Service-Type = Outbound-User
   Reply-Message = "Up to 16 lines of up to 80 characters each",
   Reply-Message = "will be accepted. Long lines will be truncated",
   Reply-Message = "Additional lines will be ignored",
   Reply-Message = " ",
   Reply-Message = "There can be up to 10 Ascend-Host-Info entries",
   Reply-Message = "in this profile. Each entry contains an IP
address",
   Reply-Message = "to Telnet to and up to 31 characters of text",
   Reply-Message = "describing the host. The text will be assigned",
   Reply-Message = "a number. When the number is selected a telnet",
   Reply-Message = "session to the ip address will be initiated.",
   Ascend-Host-Info = "1.2.3.4 a host name or phrase",
   Ascend-Host-Info = "1.2.3.5 another host",
   Ascend-Host-Info = "5.4.3.2 the last host"

#  A D D R E S S - P O O L S   P S E U D O - U S E R S
#
#  The user pools-xxx (where xxx is the name of the requesting
#  unit) returns the pools assigned to that unit.
#
#  The Ascend-IP-Pool-Definition attribute is used to define
#  an address pool. The format of the attribute is a string
#  containing:
#
#     x h.h.h.h n
#  where:
#
#     x  Pool number. A pool is selected in a user
#        profile by putting its pool number in an
#        Ascend-Assign-IP-Pool attribute.
#
#     h.h.h.hBase ip address. This is the first address in
#        the pool.
#
#     n  Maximum number of entries from the pool.
#
pools-xxxUser-Password = "ascend", Service-Type = Outbound-User
   Ascend-IP-Pool-Definition = "1 10.1.0.1 7",
```

```
    Ascend-IP-Pool-Definition = "2 10.2.0.1 48"

#   R O U T E - n   P S E U D O - U S E R S
#
#   The format of a route entry is a string containing
#
#      h.h.h.h/nn g.g.g.g m p name
#
#   where:
#
#      h.h.h.hIP address of destination host or network
#      /nn    Optional netmask indicator.
#      g.g.g.gIP address of the gateway
#      m      Metric (number of hops) for this route.
#      p      Optional Y or Yes if route is private
#      name   Optional route name (required if dialing out)
#
#   The presence of an optional field requires ALL previous fields
#   to be present. Routes are ignored if there is no place to store
#   them in the passed information structure.
#
route-1User-Password = "ascend", Service-Type = Outbound-User
    Framed-Route = "10.0.100.0/24 10.0.100.1 1 n homer-out"

route-2User-Password = "ascend", Service-Type = Outbound-User
    Framed-Route = "10.0.200.0/24 10.0.200.1 1 n inu-out"

#   O U T D I A L   P S E U D O - U S E R S
#
#   These profiles represent standard RADIUS
#   users, but contain extra attributes associated with outgoing
#   calls. Be sure that each is protected by adding the
#   Service-Type attribute on the password line.
#

#

permconn-k-1 User-Password = "ascend" , Service-Type = Outbound-User
    Framed-Protocol = FR,
```

```
        Framed-IP-Address = 200.5.249.46,
        Framed-IP-Netmask = 255.255.255.240,
        Framed-Routing = None,
        Ascend-Route-IP = Route-IP-Yes,
        Ascend-Metric = 7,
        Ascend-FR-DLCI = 109,
        Ascend-FR-Profile-Name = "fr1",
        Idle-Timeout = 130,
        Framed-MTU = 1524,
        Ascend-PRI-Number-Type = National-Number,
        Ascend-Force-56 = Force-56-No,
        Ascend-Data-Svc = Switched-56KR,
        Ascend-Call-Type = Nailed

    permconn-k-2 User-Password = "ascend" , Service-Type = Outbound-User
        Framed-Protocol = FR,
        Framed-IP-Address = 200.5.249.164,
        Framed-IP-Netmask = 255.255.255.240,
        Framed-Routing = None,
        Ascend-Route-IP = Route-IP-Yes,
        Ascend-Metric = 7,
        Ascend-FR-DLCI = 105,
        Ascend-FR-Profile-Name = "fr1",
        Idle-Timeout = 130,
        Framed-MTU = 1524,
        Ascend-PRI-Number-Type = National-Number,
        Ascend-Force-56 = Force-56-No,
        Ascend-Data-Svc = Switched-56KR,
        Ascend-Call-Type = Nailed

    permconn-k-3 User-Password = "ascend" , Service-Type = Outbound-User
        Framed-Protocol = FR,
        Framed-IP-Address = 199.6.43.141,
        Framed-IP-Netmask = 255.255.255.0,
        Framed-Routing = None,
        Ascend-Route-IP = Route-IP-Yes,
        Ascend-Metric = 7,
        Ascend-FR-DLCI = 114,
        Ascend-FR-Profile-Name = "fr1",
```

```
        Idle-Timeout = 130,
        Framed-MTU = 1524,
        Ascend-PRI-Number-Type = National-Number,
        Ascend-Force-56 = Force-56-No,
        Ascend-Data-Svc = Switched-56KR,
        Ascend-Call-Type = Nailed

    homer-out User-Password = "ascend", Service-Type = Outbound-User
        User-Name = "homer",
        Ascend-Dial-Number = "31",
        Framed-Protocol = PPP,
        Framed-IP-Address = 10.0.100.1,
        Framed-IP-Netmask = 255.255.255.0,
        Ascend-Metric = 2,
        Framed-Routing = None,
        Framed-Route = "10.5.0.0/24 10.0.100.1 1",
        Idle-Timeout = 30,
        Ascend-Send-Auth = Send-Auth-PAP,
        Ascend-Send-Secret = "passwrd1"

    #   Filters (a Lucent extension to RADIUS)
    #
    #   Two string fields have been defined in the RADIUS dictionary,
    #   Ascend-Data-Filter and Ascend-Call-Filter. The Ascend-Data-Filter
    #   defines a data/routing filter. An Ascend-Call-Filter defines a
    #   "place a call and/or keep a call active" filter.
    #
    #   Keywords are not case sensitive. In the following definitions
    #   [ ... ] indicates an optional element.
    #
    #   IP Filters:
    #
    #   "ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ]
    #       [ proto [ dstport cmp value ] [ srcport cmp value ] [ est ] ]"
    #
    #   where:
    #
    #   ip:    The keyword ip. This keyword indicates an IP filter.
    #
```

```
#  dir:   Filter direction, either IN or OUT.
#         IN filters packets coming into the Lucent box.
#         OUT filters packets going out of the Lucent box.
#
#  action:What to do with a packet that matches the filter,
#         either FORWARD or DROP.
#
#  dstip: The optional destination IP. If it is not present, the
#         filter will match any IP address. If a netmask
#         portion (/nn) of the address is present, the unit will
#         only compare the masked bits. The keyword "dstip"
#         must proceed the IP address.
#
#  srcip: The optional source IP. If it is not present, the
#         filter will match any IP address. If a netmask
#         portion (/nn) of the address is present, the unit will
#         only compare the masked bits. The keyword "srcip"
#         must proceed the IP address.
#
#
#  proto: The optional protocol. It may be specified as either
#         a name or a number. The supported names are
#         icmp(1), tcp(6), udp(17), ospf(89).
#
#  dstport:Only valid when proto is tcp(6) or udp(17). 'cmp'
#         can have the value '<', '=', '>', or '!='. The
#         value can be entered as a number or a name.
#         Supported names are ftp-data(20), ftp(21),
#         telnet(23), smpt(25), nameserver(42), domain(53),
#         tftp(69), gopher(70), finger(79), www(80),
#         kerberos(88), hostname(101), nntp(119), ntp(123),
#         exec(512), login(513), cmd(514), and talk(517).
#         The field matches any port when not present. The keyword
#         "dstport" must proceed 'cmp'.
#
#  srcport:Only valid when proto is tcp(6) or udp(17). 'cmp'
#         can have the value '<', '=', '>', or '!='. The
#         value can be entered as a number or a name.
#         Supported names are ftp-data(20), ftp(21),
```

```
#         telnet(23), smpt(25), nameserver(42), domain(53),
#         tftp(69), gopher(70), finger(79), www(80),
#         kerberos(88), hostname(101), nntp(119), ntp(123),
#         exec(512), login(513), cmd(514), and talk(517).
#         The field matches any port when not present. The keyword
#         "srcport" must proceed 'cmp'.
#
#  est:   The optional keyword EST. It is only valid when the proto
#         field is tcp(6).
#
#  GENERIC filters:
#
#
#  "generic dir action offset mask value [ more ]"
#
#  where:
#
#  generic:The keyword "generic". This keyword is used to indicate a
#              generic filter.
#
#  dir:   Filter direction, either IN or OUT.
#         IN filters packets coming into the Lucent box.
#         OUT filters packets going out of the Lucent box.
#
#  action:What to do with a packet that matches the filter.
#         (either FORWARD or DROP).
#
#  offset:A number that specifies an offset into a frame.
#
#  mask:  A hexadecimal mask of bits to compare. A one bit
#         in the mask indicates a bit to compare. Zero bits
#         are ignored. The length of the mask specifies the
#         length of the comparison. The mask may not exceed
#         6 bytes (12 hexadecimal digits).
#
#  value: The value to compare with the masked data at the offset
#         in the packet. Note: The length of the value must
#         be the same as the mask or the entry will be
#         ignored.
```

```
#
#  comparison:'==' or '!=', for Equal or NotEqual. No
#         comparison field means Equal.
#
#  more:  The optional keyword MORE. If present, the keyword
#         specifies that the next filter entry is to be applied to
#         the current packet. The <dir> and <action> of the
#         next entry must be the same as the <dir> and <action>
#         of the current entry or the MORE flag will be
#         ignored.
#
#  In the following example, the profile allows IP and ARP output,
#  but drop all other packets.
#
inu-out User-Password = "ascend", Service-Type = Outbound-User
    User-Name = "inu",
    Ascend-Dial-Number = 555-1234,
    Framed-IP-Address = 10.0.200.1,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Metric = 1,
    Framed-Routing = None,
    Idle-Timeout = 20,
    Ascend-Send-Auth = Send-Auth-CHAP,
    Ascend-Send-Secret = "kuro",
    Ascend-Data-Filter = "ip out forward",
    Ascend-Data-Filter = "generic out forward 12 ffff 0806",
    Ascend-Data-Filter = "generic out drop 0 0 0"


#  C L I D   A U T H E N T I C A T I O N
#
#  CLID entries have a "name" set to the incoming phone number and
#  and a constant password of "Ascend-CLID". The real name should
#  be placed in the profile.
#
5551212User-Password = "Ascend-CLID", Service-Type = Outbound-User
    User-Name = "real-user-name",
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.10.0.1,
```

```
    Framed-IP-Address = 255.255.255.0


#   D E F A U L T S
#
#   Note: Only one of these may be used, and it must be
#   the last entry in the file.
#
#   The following entry allows a terminal-server user to log in using a
#   UNIX account name and password.
#
DEFAULTUser-Password = "UNIX"
    Service-Type = Login-User,
    Login-Service = Telnet

#   The following entry allows a PPP user to log in using an account
#   name and SafeWord dynamic password.
#
#DEFAULTUser-Password = "SAFEWORD"
#   Service-Type = Framed-User,
#   Framed-Protocol = PPP,
#   Framed-IP-Address = 10.20.0.1,
#   Framed-IP-Netmask = 255.255.255.0
```

Disconnect/Progress Code Combinations

C

The TAOS unit applies a Disconnect code and Progress code to each call. Table C-1 provides a partial list of code combinations and their possible causes. For a complete list of Disconnect codes, see “Ascend-Disconnect-Cause (195)” on page 4-57. For a complete list of Progress codes, see “Ascend-Connect-Progress (196)” on page 4-42.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
4	101	Before the call was answered, it failed to provide a Calling-Line ID (CLID) configured on the TAOS unit.
10	31	The TAOS unit’s modem detected a training failure before the phone line disconnected. The cause might be one of the following: • During modem training, the TAOS unit waited for the Data Carrier Detect (DCD) signal from the user’s modem, but never detected the signal because the modems had marginal line quality. Because the TAOS unit’s modem has a digital connection to its local Central Office (CO), the poor line quality occurred between the user’s modem and its local CO. • A user tested the availability of the TAOS unit by dialing into the TAOS unit, and then hanging up during modem training. • There might be an incompatibility between the modems.
11	30	During modem training, the TAOS unit’s modem detected DCD but lost the modem carrier signal, usually because the modems had marginal line quality. Because the TAOS unit’s modem has a digital connection to its local CO, the poor line quality occurred between the user’s modem and its local CO. The problem might also have been caused by an incompatibility between the modems.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
11	40	During an active terminal-server session, the TAOS unit lost the carrier signal from the user's modem. The call could have ended normally, or the modems might have had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
11	43	During an active raw TCP session, the TAOS unit's modem lost the carrier signal that a modem connection requires. The call could have ended normally, or the modems might have had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
11	60	While the session was active, the TAOS unit's modem lost the carrier signal that a modem connection requires. Some client applications do not close PPP connections gracefully, so this combination might be a normal end to a customer call. Or, the modems might have had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
11	65	During PPP negotiation, the TAOS unit's modem lost the carrier signal that a modem connection requires. Typically, the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
21	40	During a terminal-server session, the TAOS unit disconnected the call because its terminal server timed out waiting for a response from the dial-in user.
24	43	During an active raw TCP session, the TAOS unit received a forced disconnect from the dial-in client's terminal-server application. Typically, the session was successful.
25	40	During an active terminal-server session, the user failed to log in successfully within the maximum number of attempts.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
27	40	During an active terminal-server session, the user pressed <ctrl>, then the Enter key, manually ending the terminal-server session and the connection. Typically, the session was successful.
35	60	During an active session, the TAOS unit stopped receiving the MP+ management packets that indicate that the line is active but idle. Typically, this code combination indicates that there was a problem with the MP+ connection.
40	75	During LCP negotiation, the TAOS unit disconnected the call because the dial-in client stopped sending LCP configuration frames. Some PPP applications require a user to press a key to continue LCP negotiation. If the user does not press a key to continue, the negotiation stops.
42	65	The dial-in client and the TAOS unit successfully negotiated LCP. The dial-in client's PPP application (or the user) supplied an incorrect user name or password during Password Authentication Protocol (PAP) authentication.
42	200	The dial-in client connected successfully to the TAOS unit, but the authentication server was not available to process the request from the TAOS unit. The authentication server might be disabled or turned off.
43	65	The TAOS unit and the dial-in client had negotiated CHAP authentication. The TAOS unit disconnected the call when the user (or the dial-in client's PPP application) supplied an incorrect username or password.
45	60	While the session was active, the TAOS unit received a Terminate Request message from the user's PPP application. Typically, the session was successful, and the user disconnected the session from the dial-in client's PPP application.
45	63	After successfully completing LCP negotiation and authentication, the TAOS unit received a Terminate Request message from the dial-in client's PPP application. For an IP-routed connection, there might be an IP address assignment misconfiguration. If you configure the TAOS unit to supply an IP address and the dial-in client does not accept the assignment, the connection clears.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
45	65	Before the initial connection was active (during PPP negotiation), the TAOS unit received a Terminate Request from the user's PPP application. Typically, the user has manually disconnected the call from the dial-in client before the PPP negotiation had completed between the dial-in client and the TAOS unit.
45	66	After successfully negotiating PPP Compression Control Protocol (CCP), the TAOS unit received a Terminate Request from the user's PPP application. Typically, the user has disconnected the session from the dial-in client's PPP application.
46	60	During an active PPP session, the TAOS unit received a Close Request from the dial-in client, resulting in a graceful disconnect. Typically, the session was successful.
47	60	Both the TAOS unit and the dial-in client successfully negotiated PPP, but no Network Control Protocols (NCPs) were successfully negotiated. Both the TAOS unit and the dial-in client must be configured to successfully negotiate at least one NCP.
47	63	The TAOS unit successfully completed LCP negotiation and authentication. The configuration of the user's PPP application did not match the TAOS unit's PPP configuration. The two devices could not successfully negotiate any Network Control Protocols (NCPs). Both the TAOS unit and the dial-in client must be configured to successfully negotiate at least one NCP.
100	60	While the session was active, the TAOS unit disconnected the call because of a configured session timeout parameter. Typically, the session was successful.
100	65	During PPP negotiation, the TAOS unit disconnected the call because of a configured session timeout parameter.
101	67	The TAOS unit successfully negotiated LCP and authentication with the dial-in client. The TAOS unit disconnected the call during IP routing (IPCP) negotiation, which typically occurs because a) the computer's IP address (configured on the TAOS unit) does not match the configuration of the IP address of the dial-in client, or b) the TAOS unit has no available IP address from its pool to assign to dial-in client.
106	60	During an active session, the TAOS unit disconnected the call because of a Multilink PPP (MP) session timeout.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
120	30	The TAOS unit received the call and allocated a modem to answer it. The dial-in client requested a protocol that is either disabled or unsupported on the TAOS unit or its modem.
181	10	The TAOS unit received and answered the incoming call. Because of inferior line quality or modem incompatibilities, the TAOS unit disconnected the call. Typically, the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO.
185	10	Shortly after answering the call, the TAOS unit could not detect any signal from the computer's modem, probably because the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
185	30	The TAOS unit received the user's modem call and allocated a modem to answer the call. Before completing modem negotiation, the TAOS unit could not detect any signal from the user's computer modem, probably because the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
185	31	Rather than indicating that the TAOS unit's modem detected a training failure, this code combination indicates that the phone line disconnected *before* the TAOS unit's modem could detect the training failure. Typically, the problem occurred because the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
185	40	During an active terminal-server session, the user probably turned off the computer or manually disconnected the WAN line from the computer's modem, resulting in an ungraceful disconnect. Typically, the session was successful. The problem might also have been caused by an incompatibility between the modems.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
185	43	During an active raw TCP session, the user probably turned off the computer or manually disconnected the WAN line from the computer's modem, resulting in an ungraceful disconnect. Typically, the session was successful. The problem might also have been caused by an incompatibility between the modems.
185	60	Instead of disconnecting the call from within the PPP application, the user probably turned off the computer or manually disconnected the WAN line from the computer, resulting in an ungraceful disconnect. Typically, the session was successful. The problem might also have been caused by an incompatibility between the modems.
185	63	Typically caused when the TAOS unit does not have an available IP address to assign to the dial-in client.
185	65	Before the initial connection was active, the TAOS unit received an ungraceful disconnect from the user's computer during PPP negotiation. The user probably turned off the computer or manually disconnected the WAN line from the computer before PPP negotiations had completed. The problem might also have been caused by an incompatibility between the modems.
185	75	After having sent an LCP request, the TAOS unit could not detect any signal from the user's computer's modem, probably because the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
185	77	The TAOS unit successfully completed LCP negotiation. Before beginning the authentication phase of PPP negotiation, the TAOS unit could not detect any signal from the user's computer's modem, probably because the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.

Table C-1. Disconnect/Progress code combinations

Disconnect code	Progress code	Possible cause
185	203	The TAOS unit could not detect any signal from the computer's modem during authentication, probably because the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality occurred between the user's modem and its local CO. The problem might also have been caused by an incompatibility between the modems.
210	60	During an active session, the TAOS unit modem slot card stopped working.

Index

A

accounting
  checkpoint records 1-19
  classifying user sessions 1-26
  dynamic IP addressing, and 1-25
  Failure-to-start records in 3-10
  generating RADIUS accounting IDs 1-19
  optional tasks for system-wide 1-15
  per-user example 1-24
  required tasks for system-wide 1-14
  sample records in 3-13
  setting up on per-user basis 1-22
  setting up system-wide 1-14
  specifying numeric base for session ID 1-17
  specifying reset time 1-18
  specifying retry limit 1-16
  specifying session-report interval 1-17
  specifying source for RADIUS requests 1-16
  specifying timeout value 1-16
  specifying whether to send second Stop record 1-19
  specifying whether to send Stop packets when authentication fails 1-19
  specifying whether to send Stop packets without user name 1-18
  Start records 3-2
  Stop records 3-4
  system-wide example 1-20
Acct-Authentic (45)
  description/usage of 4-1
  Start records, in 3-2
  Stop records, in 3-4
Acct-Delay-Time (41)
  description/usage of 4-2
  Failure-to-start records, in 3-10
  Start records, in 3-2
  Stop records, in 3-5
Acct-Input-Octets (42)
  description/usage of 4-2
  Stop records, in 3-5
Acct-Input-Packets (47)
  description/usage of 4-3
  Stop records, in 3-5
Acct-Link-Count (51)
  description/usage of 4-3
  Stop records, in 3-5
Acct-Multi-Session-Id (50)
  description/usage of 4-3
  Stop records, in 3-5
Acct-Output-Octets (43)
  description/usage of 4-4
  Stop records, in 3-5
Acct-Output-Packets (48)
  description/usage of 4-4
  Stop records, in 3-5
Acct-Session-Id (44)
  Ascend-Change-Filters-Request attribute A-10
  Ascend-Disconnect-Request attribute A-10
  description/usage of 4-4
  Failure-to-start records, in 3-10
  Start records, in 3-2
  Stop records, in 3-6
Acct-Session-Time (46)
  description/usage of 4-5
  Stop records, in 3-6
Acct-Status-Type (40)
  description/usage of 4-5
  Failure-to-start records, in 3-10
  Start records, in 3-3
  Stop records, in 3-6
ACE authentication 2-13
arguments 4-7
  Ascend-Appletalk-Route 4-7
  Ascend-Bridge-Address 4-23
  Ascend-Call-Filter 4-29, 4-30
  Ascend-Data-Filter 4-45, 4-47
  Ascend-Filter 4-72
  Ascend-IP-Pool-Definition (217) 4-93
  Ascend-IPX-Route (174) 4-99
  Ascend-Menu-Item 4-102
  Ascend-PW-Expiration 4-119
  Framed-Route (22) 4-151
Ascend-Add-Seconds (240)
  Access-Accept attribute A-3
  description/usage of 4-5
Ascend-Appletalk-Peer-Mode (117)
  Access-Accept attribute A-3
  description/usage of 4-6
Ascend-Appletalk-Route (116) 4-7
  Access-Accept attribute A-3
  description/usage of 4-7
Ascend-ARA-PW (181)
  Access-Accept attribute A-3

description/usage of 4-8
Ascend-Assign-IP-Client (144)
Access-Accept attribute A-3
description/usage of 4-9
Ascend-Assign-IP-Global-Pool (146)
Access-Accept attribute A-4
description/usage of 4-9
Ascend-Assign-IP-Pool (218)
Access-Accept attribute A-4
description/usage of 4-10
Ascend-Assign-IP-Server (145)
Access-Accept attribute A-4
description/usage of 4-10
Ascend-ATM-Connect-Group (63)
Access-Accept attribute A-4
description/usage of 4-10
Ascend-ATM-Connect-Vci (62)
Access-Accept attribute A-4
description/usage of 4-11
Ascend-ATM-Connect-Vpi (61)
Access-Accept attribute A-4
description/usage of 4-11
Ascend-ATM-Direct (76)
Access-Accept attribute A-4
description/usage of 4-12
Ascend-ATM-Direct-Profile (77)
Access-Accept attribute A-4
description/usage of 4-12
Ascend-ATM-Fault-Management (14)
Access-Accept attribute A-4
description/usage of 4-13
Ascend-ATM-Group (64)
Access-Accept attribute A-4
description/usage of 4-14
Ascend-ATM-Loopback-Cell-Loss (15)
Access-Accept attribute A-4
description/usage of 4-14
Ascend-ATM-Vci (95)
Access-Accept attribute A-4
description/usage of 4-15
Ascend-ATM-Vpi (94)
Access-Accept attribute A-4
description/usage of 4-15
Ascend-Authen-Alias (203)
Access-Accept attribute A-4
description/usage of 4-16
Ascend-Auth-Type (81)
Access-Accept attribute A-4
description/usage of 4-16
Ascend-Backup (176)
Access-Accept attribute A-4
description/usage of 4-17
Ascend-BACP-Enable (133)
Access-Accept attribute A-4
description/usage of 4-18
Ascend-Base-Channel-Count (172)
Access-Accept attribute A-4
description/usage of 4-18
Ascend-Bi-Directional-Auth (46)
Access-Accept attribute A-4
description/usage of 4-19
Ascend-Billing-Number (249)
Access-Accept attribute A-4
description/usage of 4-20
Ascend-BIR-Bridge-Group (72)
Access-Accept attribute A-4
description/usage of 4-21
Ascend-BIR-Enable (70)
Access-Accept attribute A-4
description/usage of 4-21
Ascend-BIR-Proxy (71)
Access-Accept attribute A-4
description/usage of 4-22
Ascend-Bridge (230)
Access-Accept attribute A-4
description/usage of 4-22
Ascend-Bridge-Address (168)
Access-Accept attribute A-4
arguments 4-23
description/usage of 4-23
Ascend-Bridge-Non-PPPoE (75)
Access-Accept attribute A-4
description/usage of 4-24
Ascend-Cache-Refresh (56)
Access-Accept attribute A-4
description/usage of 4-24
Ascend-Cache-Time (57)
Access-Accept attribute A-4
description/usage of 4-25
Ascend-Call-Attempt-Limit (123)
Access-Accept attribute A-4
description/usage of 4-25
Ascend-Callback (246)
Access-Accept attribute A-4
description/usage of 4-26
Ascend-Callback-Delay (108)
Access-Accept attribute A-4
description/usage of 4-26
Ascend-Call-Block-Duration (124)
Access-Accept attribute A-4
description/usage of 4-27
Ascend-Call-By-Call (250)
Access-Accept attribute A-4
description/usage of 4-27
Ascend-Call-Filter (243)
Access-Accept attribute A-4
arguments 4-29, 4-30
Ascend-Change-Filters-Request attribute A-10

description/usage of 4-28
Ascend-Calling-Id-Numbering-Plan (67)
Access-Request attribute A-2
description/usage of 4-32
Ascend-Calling-Id-Presentation (68)
Access-Request attribute A-2
description/usage of 4-32
Ascend-Calling-Id-Screening (69)
Access-Request attribute A-2
description/usage of 4-33
Ascend-Calling-Id-Type-Of-Number (66)
Access-Request attribute A-2
description/usage of 4-34
Ascend-Calling-Subaddress (107)
Access-Request attribute A-2
description/usage of 4-34
Start records, in 3-3
Stop records, in 3-6
Ascend-Call-Type (177)
Access-Accept attribute A-4
description/usage of 4-35
Ascend-CBCP-Delay (114), unused attribute 4-171
Ascend-CBCP-Enable (112)
Access-Accept attribute A-4
description/usage of 4-37
Ascend-CBCP-Mode (113)
Access-Accept attribute A-4
description/usage of 4-37
Ascend-CBCP-Trunk-Group (115)
Access-Accept attribute A-4
description/usage of 4-38
Ascend-Ckt-Type (16)
Access-Accept attribute A-4
description/usage of 4-38
Ascend-Client-Assign-DNS (137)
Access-Accept attribute A-5
description/usage of 4-39
Ascend-Client-Assign-WINS (80)
Access-Accept attribute A-5
description/usage of 4-39
Ascend-Client-Primary-DNS (135)
Access-Accept attribute A-5
description/usage of 4-40
Ascend-Client-Primary-WINS (78)
Access-Accept attribute A-5
description/usage of 4-41
Ascend-Client-Secondary-DNS (136)
Access-Accept attribute A-5
description/usage of 4-41
Ascend-Client-Secondary-WINS (79)
Access-Accept attribute A-5
description/usage of 4-42
Ascend-Connect-Progress (196)
codes 4-43
description/usage of 4-42
Failure-to-start records, in 3-10
Stop records, in 3-6
Ascend-Data-Filter (242)
Access-Accept attribute A-5
arguments 4-45, 4-47
Ascend-Change-Filters-Request attribute A-10
description/usage of 4-45
Ascend-Data-Rate (197)
Access-Request attribute A-2
description/usage of 4-49
Failure-to-start records, in 3-10
Stop records, in 3-6
Ascend-Data-Svc (247)
Access-Accept attribute A-5
description/usage of 4-49
Ascend-DBA-Monitor (171)
Access-Accept attribute A-5
description/usage of 4-53
Ascend-Dec-Channel-Count (237)
Access-Accept attribute A-5
description/usage of 4-54
Ascend-DHCP-Maximum-Leases (134)
Access-Accept attribute A-5
description/usage of 4-55
Ascend-DHCP-Pool-Number (148)
Access-Accept attribute A-5
description/usage of 4-55
Ascend-DHCP-Reply (147)
Access-Accept attribute A-5
description/usage of 4-56
Ascend-Dial-Number (227)
Access-Accept attribute A-5
description/usage of 4-57
Start records, in 3-3
Stop records, in 3-6
Ascend-Dialout-Allowed (131)
Access-Accept attribute A-5
description/usage of 4-56
Ascend-Disconnect-Cause (195)
description/usage of 4-57
Failure-to-start records, in 3-10
Stop records, in 3-6
Ascend-Dsl-CIR-Recv-Limit (100)
Access-Accept attribute A-5
description/usage of 4-64
Ascend-Dsl-CIR-Xmit-Limit (101)
Access-Accept attribute A-5
description/usage of 4-65
Ascend-DSL-Downstream-Limit (99)
Access-Accept attribute A-5
description/usage of 4-65
Ascend-Dsl-Rate-Mode (97)
Access-Accept attribute A-5

description/usage of 4-67
Ascend-Dsl-Rate-Type (92)
Access-Accept attribute A-5
description/usage of 4-67
Ascend-DSL-Upstream-Limit (98)
Access-Accept attribute A-5
description/usage of 4-68
Ascend-Egress-Enabled (58)
Access-Accept attribute A-5
description/usage of 4-69
Ascend-Endpoint-Disc (109)
Access-Accept attribute A-5
description/usage of 4-70
Ascend-Event-Type (150)
Ascend-Access-Event-Request attribute A-9
Ascend-Access-Event-Response attribute A-9
description/usage of 4-70
Stop records, in 3-6
Ascend-Expect-Callback (149)
Access-Accept attribute A-5
description/usage of 4-71
Ascend-FCP-Parameter (119)
Access-Accept attribute A-5
description/usage of 4-71
Ascend-Filter (91)
Access-Accept attribute A-5
arguments 4-72
description/usage of 4-71
Ascend-Filter-Required (50)
Access-Accept attribute A-5
description/usage of 4-74
Ascend-First-Dest (189)
Access-Accept attribute A-5
description/usage of 4-74
Stop records, in 3-7
Ascend-Force-56 (248)
Access-Accept attribute A-5
description/usage of 4-75
Ascend-FR-08-Mode (10)
Access-Accept attribute A-5
description/usage of 4-75
Ascend-FR-Circuit-Name (156)
Access-Accept attribute A-5
description/usage of 4-76
Ascend-FR-DCE-N392 (162)
Access-Accept attribute A-5
description/usage of 4-76
Ascend-FR-DCE-N393 (164)
Access-Accept attribute A-5
description/usage of 4-77
Ascend-FR-Direct (219)
Access-Accept attribute A-5
description/usage of 4-77
Ascend-FR-Direct-DLCI (221)
Access-Accept attribute A-5
description/usage of 4-78
Ascend-FR-Direct-Profile (220)
Access-Accept attribute A-5
description/usage of 4-78
Ascend-FR-DLCI (179)
Access-Accept attribute A-5
description/usage of 4-79
Ascend-FR-DTE-N392 (163)
Access-Accept attribute A-5
description/usage of 4-79
Ascend-FR-DTE-N393 (165)
Access-Accept attribute A-5
description/usage of 4-80
Ascend-FR-Link-Mgt (160)
Access-Accept attribute A-6
description/usage of 4-80
Ascend-FR-Link-Status-DLCI (106)
Access-Accept attribute A-6
description/usage of 4-81
Ascend-FR-LinkUp (157), unused attribute 4-171
Ascend-FR-N391 (161)
Access-Accept attribute A-6
description/usage of 4-81
Ascend-FR-Nailed-Grp (158)
Access-Accept attribute A-6
description/usage of 4-82
Ascend-FR-Profile-Name (180)
Access-Accept attribute A-6
description/usage of 4-82
Ascend-FR-SVC-Addr (13)
Access-Accept attribute A-6
description/usage of 4-82
Ascend-FR-T391 (166)
Access-Accept attribute A-6
description/usage of 4-83
Ascend-FR-T392 (167)
Access-Accept attribute A-6
description/usage of 4-83
Ascend-FR-Type (159)
Access-Accept attribute A-6
description/usage of 4-84
Ascend-FT1-Caller (175)
Access-Accept attribute A-6
description/usage of 4-85
Ascend-Group (178)
Access-Accept attribute A-6
description/usage of 4-85
Ascend-Handle-IPX (222)
Access-Accept attribute A-6
description/usage of 4-86
Ascend-History-Weigh-Type (239)
Access-Accept attribute A-6
description/usage of 4-87

Ascend-Home-Agent-IP-Addr (183)
description/usage of 4-88
Stop records, in 3-7
Ascend-Home-Agent-UDP-Port (186)
Access-Accept attribute A-6
description/usage of 4-89
Stop records, in 3-7
Ascend-Home-Network-Name (185)
Access-Accept attribute A-6
description/usage of 4-89
Stop records, in 3-7
Ascend-Host-Info (252)
Access-Accept attribute A-6
description/usage of 4-90
Ascend-IF-Netmask (153)
Access-Accept attribute A-6
description/usage of 4-90
Ascend-Inc-Channel-Count (236)
Access-Accept attribute A-6
description/usage of 4-91
Ascend-IP-Direct (209)
Access-Accept attribute A-6
description/usage of 4-91
Ascend-IP-Pool-Chaining (85)
Access-Accept attribute A-6
description/usage of 4-92
Ascend-IP-Pool-Definition (217)
Access-Accept attribute A-6
arguments 4-93
description/usage of 4-93
Ascend-IPSEC-Profile (73)
Access-Accept attribute A-6
description/usage of 4-94
Ascend-IP-TOS (88)
Access-Accept attribute A-6
description/usage of 4-94
Ascend-IP-TOS-Apply-To (90)
Access-Accept attribute A-6
description/usage of 4-95
Ascend-IP-TOS-Precedence (89)
Access-Accept attribute A-6
description/usage of 4-96
Ascend-IPX-Alias (224)
Access-Accept attribute A-6
description/usage of 4-96
Ascend-IPX-Header-Compression (65)
Access-Accept attribute A-6
description/usage of 4-97
Ascend-IPX-Node-Addr (182)
Access-Accept attribute A-6
description/usage of 4-97
Ascend-IPX-Peer-Mode (216)
Access-Accept attribute A-6
description/usage of 4-98
Ascend-IPX-Route (174)
Access-Accept attribute A-6
arguments 4-99
description/usage of 4-98
Ascend-Link-Compression (233)
Access-Accept attribute A-6
description/usage of 4-99
Ascend-Maximum-Call-Duration (125)
Access-Accept attribute A-6
description/usage of 4-100
Ascend-Maximum-Channels (235)
Access-Accept attribute A-6
description/usage of 4-101
Ascend-Menu-Item (206)
Access-Accept attribute A-6
arguments 4-102
description/usage of 4-102
Ascend-Menu-Selector (205)
Access-Accept attribute A-6
description/usage of 4-103
Ascend-Metric (225)
Access-Accept attribute A-6
description/usage of 4-103
Ascend-Minimum-Channels (173)
Access-Accept attribute A-6
description/usage of 4-104
Ascend-Modem-PortNo (120)
description/usage of 4-104
Start records, in 3-3
Stop records, in 3-7
Ascend-Modem-ShelfNo (122)
description/usage of 4-105
Start records, in 3-3
Stop records, in 3-7
Ascend-Modem-SlotNo (121)
description/usage of 4-105
Start records, in 3-3
Stop records, in 3-7
Ascend-MPP-Idle-Percent (254)
Access-Accept attribute A-6
description/usage of 4-105
Ascend-MTU (49)
Access-Accept attribute A-6
description/usage of 4-106
Ascend-Multicast-Client (155)
Access-Accept attribute A-7
description/usage of 4-106
Ascend-Multicast-GLeave-Delay (111)
Access-Accept attribute A-7
description/usage of 4-107
Ascend-Multicast-Rate-Limit (152)
Access-Accept attribute A-7
description/usage of 4-108
Ascend-Multilink-ID (187)

Access-Accept attribute A-7
description/usage of 4-108
Stop records, in 3-7
Ascend-Netware-timeout (223)
Access-Accept attribute A-7
description/usage of 4-108
Ascend-Numbering-Plan-ID (105)
Access-Accept attribute A-7
description/usage of 4-109
Ascend-Number-Sessions (202)
Ascend-Access-Event-Request attribute A-9
Ascend-Access-Event-Response attribute A-9
description/usage of 4-110
Stop records, in 3-7
Ascend-Num-In-Multilink (188)
Access-Accept attribute A-7
description/usage of 4-110
Stop records, in 3-7
Ascend-Owner-IP-Addr (86)
description/usage of 4-110
Start records, in 3-3
Stop records, in 3-7
Ascend-Port-Redir-Portnum (83)
Access-Accept attribute A-7
description/usage of 4-111
Ascend-Port-Redir-Protocol (82)
Access-Accept attribute A-7
description/usage of 4-111
Ascend-Port-Redir-Server (84)
Access-Accept attribute A-7
description/usage of 4-112
Ascend-PPP-Address (253)
Access-Accept attribute A-7
description/usage of 4-112
Ascend-PPP-Async-Map (212)
Access-Accept attribute A-7
description/usage of 4-112
Ascend-PPPoE-Enable (74)
Access-Accept attribute A-7
description/usage of 4-113
Ascend-PPP-VJ-1172 (211)
Access-Accept attribute A-7
description/usage of 4-113
Ascend-PPP-VJ-Slot-Comp (210)
Access-Accept attribute A-7
description/usage of 4-114
Ascend-Preempt-Limit (245)
Access-Accept attribute A-7
description/usage of 4-114
Ascend-Pre-Input-Octets (190)
Access-Accept attribute A-7
description/usage of 4-115
Stop records, in 3-8
Ascend-Pre-Input-Packets (192)
Access-Accept attribute A-7
description/usage of 4-115
Stop records, in 3-8
Ascend-Pre-Output-Octets (191)
Access-Accept attribute A-7
description/usage of 4-116
Stop records, in 3-8
Ascend-Pre-Output-Packets (193)
Access-Accept attribute A-7
description/usage of 4-116
Stop records, in 3-8
Ascend-PreSession-Time (198)
description/usage of 4-116
Failure-to-start records, in 3-10
Stop records, in 3-8
Ascend-PRI-Number-Type (226)
Access-Accept attribute A-7
description/usage of 4-117
Ascend-Private-Route (104)
Access-Accept attribute A-7
description/usage of 4-117
Ascend-Private-Route-Required (55)
Access-Accept attribute A-7
description/usage of 4-118
Ascend-Private-Route-Table-ID (54)
Access-Accept attribute A-7
description/usage of 4-119
Ascend-PW-Expiration (21)
Access-Accept attribute A-7
arguments 4-119
description/usage of 4-119
Ascend-PW-Lifetime (208)
Access-Accept attribute A-7
description/usage of 4-120
Ascend-PW-Warntime (207)
Access-Accept attribute A-7
description/usage of 4-120
Ascend-QOS-Downstream (60)
Access-Accept attribute A-7
description/usage of 4-121
Ascend-QOS-Upstream (59)
Access-Accept attribute A-7
description/usage of 4-121
Ascend-Receive-Secret (215)
Access-Accept attribute A-7
description/usage of 4-122
Ascend-Recv-Name (45)
Access-Accept attribute A-7
description/usage of 4-122
Ascend-Redirect-Number (109)
description/usage of 4-123
Start records, in 3-3
Stop records, in 3-8
Ascend-Remote-Addr (154)

Access-Accept attribute A-7
description/usage of 4-123
Ascend-Remote-FW (110)
Access-Accept attribute A-7
description/usage of 4-124
Ascend-Remove-Seconds (241)
Access-Accept attribute A-7
description/usage of 4-124
Ascend-Require-Auth (201)
Access-Accept attribute A-7
description/usage of 4-125
Ascend-Route-Appletalk (118)
Access-Accept attribute A-7
description/usage of 4-126
Ascend-Route-IP (228)
Access-Accept attribute A-7
description/usage of 4-126
Ascend-Route-IPX (229)
Access-Accept attribute A-7
description/usage of 4-127
Ascend-Route-Preference (126)
Access-Accept attribute A-7
description/usage of 4-127
Ascend-Secondary-Home-Agent (130)
Access-Accept attribute A-8
description/usage of 4-128
Ascend-Seconds-Of-History (238)
Access-Accept attribute A-8
description/usage of 4-129
Ascend-Send-Auth (231)
Access-Accept attribute A-8
description/usage of 4-130
Ascend-Send-Passwd (232)
Access-Accept attribute A-8
Access-Request attribute A-2
description/usage of 4-131
Ascend-Send-Secret (214)
Access-Accept attribute A-8
Access-Request attribute A-2
description/usage of 4-131
Ascend-Session-Svr-Key (151)
Ascend-Change-Filters-Request attribute A-10
Ascend-Disconnect-Request attribute A-10
description/usage of 4-132
Start records, in 3-3
Ascend-Shared-Profile-Enable (128)
Access-Accept attribute A-8
description/usage of 4-132
Ascend-Source-Auth (103)
Access-Accept attribute A-8
description/usage of 4-133
Ascend-Source-IP-Check (96)
Access-Accept attribute A-8
description/usage of 4-134
Ascend-SVC-Enabled (17)
Access-Accept attribute A-8
description/usage of 4-134
Ascend-Target-Util (234)
Access-Accept attribute A-8
description/usage of 4-134
Ascend-Telnet-Profile (91)
Access-Accept attribute A-8
description/usage of 4-135
Ascend-Third-Prompt (213)
Access-Accept attribute A-8
description/usage of 4-136
Ascend-Token-Expiry (204)
Access-Accept attribute A-8
description/usage of 4-136
Ascend-Token-Idle (199)
Access-Accept attribute A-8
description/usage of 4-136
Ascend-Token-Immediate (200)
Access-Accept attribute A-8
description/usage of 4-137
Ascend-Traffic-Shaper (51)
Access-Accept attribute A-8
description/usage of 4-137
Ascend-Transit-Number (251)
Access-Accept attribute A-8
description/usage of 4-138
Ascend-TS-Idle-Limit (169)
Access-Accept attribute A-8
description/usage of 4-139
Ascend-TS-Idle-Mode (170)
Access-Accept attribute A-8
description/usage of 4-139
Ascend-Tunnel-VRouter-Name (31)
Access-Accept attribute A-8
description/usage of 4-140
Ascend-User-Acct-Base (142)
description/usage of 4-140
Start records, in 3-3
Stop records, in 3-8
Ascend-User-Acct-Host (139)
description/usage of 4-140
Start records, in 3-3
Stop records, in 3-8
Ascend-User-Acct-Key (141)
description/usage of 4-141
Start records, in 3-3
Stop records, in 3-8
Ascend-User-Acct-Port (140)
description/usage of 4-141
Start records, in 3-3
Stop records, in 3-9
Ascend-User-Acct-Time (143)
description/usage of 4-142

Start records, in 3-3
Stop records, in 3-9
Ascend-User-Acct-Type (138)
description/usage of 4-143
Start records, in 3-3
Stop records, in 3-9
Ascend-VRouter-Name (102)
Access-Accept attribute A-8
description/usage of 4-143
Ascend-Xmit-Rate (255)
Access-Request attribute A-2
description/usage of 4-144
Stop records, in 3-9
AT&T settings 4-28
attributes
Access-Accept A-3
Access-Challenge A-9
Access-Password-Ack A-9
Access-Password-Expired A-9
Access-Password-Reject A-9
Access-Password-Request A-8
Access-Reject A-8
Access-Request A-2
Ascend-Access-Event-Request A-9
Ascend-Access-Event-Response A-9
Ascend-Change-Filters-Ack A-10
Ascend-Change-Filters-Nak A-10
Ascend-Change-Filters-Request A-10
Ascend-Disconnect-Ack A-10
Ascend-Disconnect-Nak A-10
Ascend-Disconnect-Request A-10
Failure-to-start records, in 3-10
listing of RADIUS 4-1
Start records, in 3-2
Stop records, in 3-4
authentication
CACHE-TOKEN 2-12
callback 2-19
CHAP 2-6
choosing method 2-1
CLID 2-2
encryption on RADIUS server 2-5
external 2-8
MS-CHAP 2-6
PAP 2-6
PAP-TOKEN 2-10
PAP-TOKEN-CHAP 2-11
PPP connections, of 2-6
RADIUS 2-1
token card 2-8
tokens, how to configure 2-8
tunnel 2-14
tunnels 2-14

C

CACHE-TOKEN authentication 2-12
callback 2-19
Callback-ID (20), not supported by TAOS 4-171
Callback-Number (19), not supported by TAOS 4-171
called-number authentication 2-2
Called-Station-Id (30)
Access-Accept attribute A-3
Access-Request attribute A-2
description/usage of 4-144
Start records, in 3-3
Stop records, in 3-9
Caller-Id (31), free-RADIUS attribute 4-170
Calling-Station-Id (31)
Access-Accept attribute A-3
Access-Request attribute A-2
description/usage of 4-145
Start records, in 3-4
Stop records, in 3-9
Challenge-Response (3), free-RADIUS attribute 4-170
Change-Password (17)
Access-Accept attribute A-3
Access-Password-Request attribute A-8
description/usage of 4-145
CHAP-Challenge (60), not supported by TAOS 4-171
CHAP-Password (3)
Access-Request attribute A-2
description/usage of 4-145
Class (25)
Access-Accept attribute A-3
Access-Request attribute A-2
description/usage of 4-145
Start records, in 3-4
Stop records, in 3-9
CLID
defined 2-2
CLID authentication 2-2
Client-Port-DNIS (30), free-RADIUS attribute 4-170

D

DNIS
defined 2-2
DNIS authentication
described 2-2

E

external authentication
servers 2-8

F

Failure-to-start records 3-10
Filter-ID (11)
  Access-Accept attribute A-3
  description/usage of 4-146
filters
  generic call filter entries 4-30
  generic data filter entries 4-47
  IP call filter entries 4-29
  IP data filter entries 4-45
Framed-Address (8), free-RADIUS attribute 4-170
Framed-AppleTalk-Link (37), not supported by TAOS 4-171
Framed-AppleTalk-Network (38), not supported by TAOS 4-171
Framed-AppleTalk-Zone (39), not supported by TAOS 4-171
Framed-Compression (13)
  Access-Accept attribute A-3
  description/usage of 4-146
Framed-IP-Address (8)
  Access-Accept attribute A-3
  Ascend-Change-Filters-Request attribute A-10
  Ascend-Disconnect-Request attribute A-10
  description/usage of 4-147
  Start records, in 3-4
  Stop records, in 3-9
Framed-IP-Netmask (9)
  Access-Accept attribute A-3
  description/usage of 4-147
Framed-IPX-Network (23)
  Access-Accept attribute A-3
  description/usage of 4-148
Framed-MTU (12)
  Access-Accept attribute A-3
  description/usage of 4-149
Framed-Netmask (9), free-RADIUS attribute 4-170
Framed-Protocol (7)
  Access-Accept attribute A-3
  Access-Request attribute A-2
  description/usage of 4-149
  Start records, in 3-4
  Stop records, in 3-9
Framed-Route (22)
  Access-Accept attribute A-3
  arguments 4-151
  description/usage of 4-151
Framed-Routing (10)
  Access-Accept attribute A-3
  description/usage of 4-152
free-RADIUS attributes, RFC equivalents and 4-170

G

generic filter, syntax elements for 4-30, 4-47

I

Idle-Timeout (28)
  Access-Accept attribute A-3
  usage/description of 4-153
IP call filter, syntax elements for 4-29
IP data filter, syntax elements for 4-45

L

Login-Host (14), free-RADIUS attribute 4-170
Login-IP-Host (14)
  Access-Accept attribute A-3
  description/usage of 4-154
Login-LAT-Group (36), not supported by TAOS 4-171
Login-LAT-Node (35), not supported by TAOS 4-171
Login-LAT-Port (63), not supported by TAOS 4-171
Login-LAT-Service (34), not supported by TAOS 4-171
Login-Service (15)
  Access-Accept attribute A-3
  description/usage of 4-155
Login-TCP-Port (16)
  Access-Accept attribute A-3
  Access-Reject attribute A-8
  description/usage of 4-155

M

MCI settings 4-28
MS-CHAP authentication 2-6
MS-CHAP-Challenge
  Access-Challenge attribute A-9
  Access-Request attribute A-2
MS-CHAP-Response
  Access-Request attribute A-2
  description/usage of 4-156

N

NAS-Identifier (32), not supported by TAOS 4-171
NAS-Identifier (4), free-RADIUS attribute 4-170
NAS-IP-Address (4)
  Access-Request attribute A-2
  Ascend-Access-Event-Request attribute A-9
  Ascend-Access-Event-Response attribute A-9

description/usage of 4-156
Failure-to-start records, in 3-10
Start records, in 3-4
Stop records, in 3-9
NAS-Port (5)
Access-Request attribute A-2
description/usage of 4-157
Start records, in 3-4
Stop records, in 3-9
NAS-Port-Type (61)
Access-Request attribute A-2
description/usage of 4-158
Start records, in 3-4
Stop records, in 3-10

P

PAP authentication, described 2-6
PAP-TOKEN-CHAP authentication
for incoming calls 2-11
Password (2), free-RADIUS attribute 4-170
password expiration attributes 2-4
passwords
changing nonexpired 2-4
encryption for dial-out 2-5
expiration 2-4
RADIUS, in 2-3
specifying expiration for 2-4
Tunnel-Password, Ascend-Home-Agent-Password, and 2-14
Port-Limit (62), not supported by TAOS 4-171
PPP
password authentication 2-6
Proxy-State (33), not supported by TAOS 4-171

R

RADIUS
authenticating Telnet session 1-11
configuring distinct ID sequences for packet IDs 1-10
customizing User-Name string 1-10
fine-tuning interaction with unit 1-9
how the unit handles User-Name attribute 1-7
password handling 2-3
returning to primary RADIUS server 1-5
Service-Type (6) not received 1-6
setting up communication with unit 1-1
specifying timeout 1-4
specifying timeout message 1-4
specifying whether remote users are dropped 1-5
specifying whether unit sends values for attributes 6 and 7 1-6
token-card server, and 2-8
VSA support 1-8
see also profiles
Reply-Message (18)
Access-Challenge attribute A-9
Access-Reject attribute A-8
description/usage of 4-159
RFC-standard attributes, not supported by TAOS 4-171

S

security
callback 2-19
CLID authentication 2-2
passwords for PPP connections 2-6
token-card authentication 2-8
using token cards 2-8
servers
Enigma Logic SafeWord 2-8
external authentication 2-8
Security Dynamics ACE/Server 2-8
Service-Type (6)
Access-Accept attribute A-3
Access-Request attribute A-2
description/usage of 4-159
Session-Timeout (27)
Access-Accept attribute A-3
description/usage of 4-160
Sprint settings 4-28
Start records 3-2
State (24)
Access-Accept attribute A-3
Access-Challenge attribute A-9
Access-Request attribute A-2
description/usage of 4-160
Stop records 3-4

T

telco
call information 2-2
token cards 2-8
access challenges 2-10
example of dial-in 2-10
token-card authentication 2-8
RADIUS, and 2-8
setting up Cache-Token 2-12
setting up PAP-Token-CHAP 2-11
token-card authentication, example 2-10
Tunnel-Assignment-ID (81), unused attribute 4-171
Tunnel-Client-Auth-ID (90)
Access-Accept attribute A-3
description/usage of 4-161

Tunnel-Client-Endpoint (66)
  description/usage of 4-161
  Stop records, in 3-10
Tunnel-ID (68)
  description/usage of 4-161
  Stop records, in 3-10
tunneling
  ATMP authentication 2-14
Tunnel-Medium-Type (65)
  Access-Accept attribute A-3
  description/usage of 4-162
Tunnel-Password (69)
  Access-Accept attribute A-3
  description/usage of 4-162
Tunnel-Preference (83)
  Access-Accept attribute A-3
  description/usage of 4-163
Tunnel-Private-Group-ID (81)
  Access-Accept attribute A-3
Tunnel-Server-Auth-ID (91), unused attribute 4-171
Tunnel-Server-Endpoint (67)
  Access-Accept attribute A-3
  description/usage of 4-165
Tunnel-Type (64)
  Access-Accept attribute A-3
  description/usage of 4-166
  Stop records, in 3-10

U

unused attributes 4-171
User-Name (1)
  Access-Password-Request attribute A-8
  Access-Request attribute A-2
  Ascend-Change-Filters-Request attribute A-10
  Ascend-Disconnect-Request attribute A-10
  description/usage of 4-167
  Start records, in 3-4
  Stop records, in 3-10
User-Password (2)
  Access-Password-Request attribute A-8
  Access-Request attribute A-2
  Ascend-Access-Event-Request attribute A-9
  description/usage of 4-168
User-Service (6), free-RADIUS attribute 4-170

V

Vendor-Specific (26)
  Access-Accept attribute A-3
  description/usage of 4-168